GDPR etterlevelse i finansbransjen

Internrevisors rolle
Hvordan kan internrevisjonen bidra?

Del 2 – Gjensidige (DPO)

Rolle; også inn mot etterlevelse
Samhandling med interne kontrollfunksjoner
Inn på erfaringer fra Gjensidige

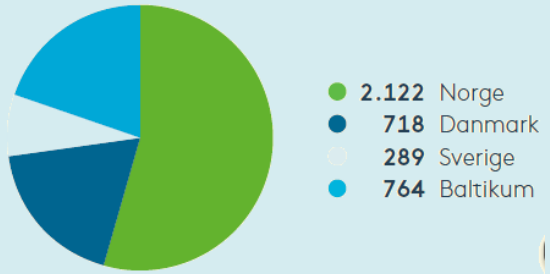
v/ Stein Kjennvold
Personvernombud i Gjensidige Forsikring ASA

06. mars 2019

Gjensidige Forsikring ASA - Et nordisk skadeforsikringskonsern

- ca 4.000 ansatte
- 6 land
- 2 filialer

Ansatte per land
per 31.12.2018



Gjensidige er et nordisk skadeforsikringskonsern. Virksomheten sikrer liv, helse og verdier for kunder i privat- og næringslivsmarkedet

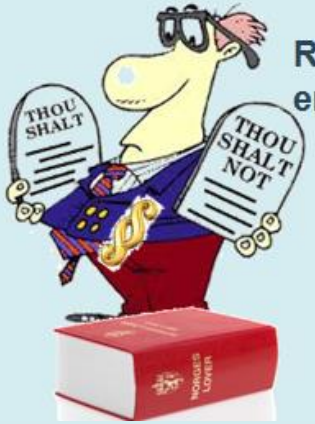
I Norge tilbys også produkter innen bank, pensjon og sparing.

Samfunnsansvar gjennom 200 år

*) Position in each country based on Q22017 Norway, Baltics and Sweden , Q32016 Denmark, and Q42016 Finland.
**) General insurance numbers are earned premiums 2016. AUM and Gross lending as of 31.12.2016

- **Kunder i Norge: ca 1 million**

Personvernombudet – hvem er det?



Rådgiveren som i realiteten er en beslutningstaker?

Personvernridderen -de registrertes kriger og den som kjemper for personvernet ?

Selskapets redningsbøye når skuta er i ferd med å gå ned?

En ny intern politibetjent?

En ny superhelt?

Den som får skylda hvis noe går galt ?

Datatilsynet

Varsel om pålegg og overtredelsesgebyr

En los som bidrar til at virksomheten og dens ansatte navigerer riktig i et kronglete farvann?

Dødelig personvern | Torkel Steen

Heldigvis bryter alle sykehusleger jeg kjenner, personvernombudets lovtolkning.

DEBATT

Forskere og leger ved Oslo universitetssykehus reagerer på ledernes tolkning av personvernreglene.

Foto: Fredrik Hagen / NTB scanpix SKJUL BILDETEKST

32 leger og forskere ut mot personverntolkning

32 forskere og leger tar et oppgjør med lederne av Oslo universitetssykehus og deres tolkning av personvernreglene.

Den vanskelige rollen som personvernombud

Debatt

Cecilie Lorvik Bødtker Rønnevik, senioradvokat, Advokatfirmaet Simonsen Vogt Wiig

Thomas Olsen , assosiert partner (PhD), Advokatfirmaet Simonsen Vogt Wiig

Personvernombudet har flere lovpålagte oppgaver. Blant annet skal ombudet gi ledelsen råd i spørsmål som angår behandling av personopplysninger. Ombudet skal også kontrollere at virksomheten faktisk etterlever personvernlovgivningen.

Ledelsen har ansvaret

Det er uansett ledelsen som har ansvar for at virksomheten opptrer i samsvar med all lovgivning, og ledelsen kan også gå imot ombudets råd.

Uavhengig og objektiv

Forordningen krever at personvernombudet opptrer uavhengig og gir ledelsen råd som er objektive og kvalifiserte. Det er forbudt å instruere ombudet om hvordan denne skal utføre sine lovpålagte oppgaver og å iverksette formelle og uformelle sanksjoner mot et ombud som utfører sine oppgaver

Risiko for konflikt

I noen virksomheter vil det oppstå dype konflikter mellom personvern og andre legitime interesser, og det er en klar risiko for at det også oppstår mer personlige konflikter mellom ombudet, ledelsen og andre ansatte. Ledelsen må derfor sørge for at ombudet får nødvendig støtte og legitimitet og samtidig være tydelige på at det er ledelsen som er rette adressat for eventuell kritikk mot de beslutninger som treffes.

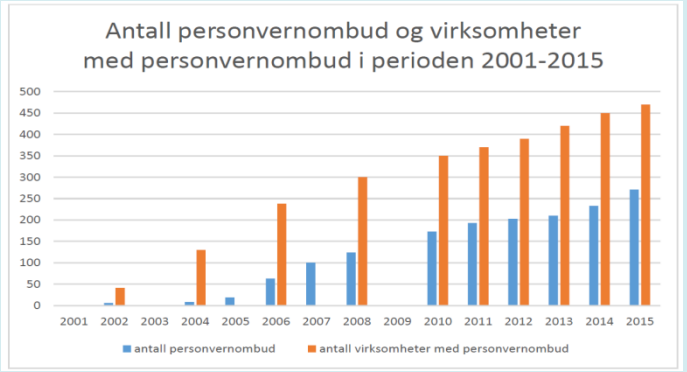
Kilde: Aftenposten

Om personvernombudsordningen

PERSONVERNOMBUD

- Etablert som en frivillig ordning i 2001 - administrert av Datatilsynet.
- Grunnlaget for opprettelsen; Personopplysningsforskriften § 7-12
- Kunne gi fritak fra meldeplikten i pol § 31, første ledd

- Tall 2017 (kilde Datatilsynet)
  - 450 personvernombud
  - 660 virksomheter med ombud



- Fremhevet og lovregulert i personvernforordningen, artikkel 37-39 og ft.97
- Skjerpede krav og tydeligere rolle
- Fra frivillig til obligatorisk ordning for mange

- Registrerte virksomheter med ombud pr 0103 2019
  - 1650

Kilde: Datatilsynet

Hvem er personvernombudsordningen obligatorisk for?

PERSONVERNOMBUD

1. offentlige myndigheter og organer (unntatt domstolene)

2. behandlingsansvarlige og databehandlere der *hovedvirksomheten* består av behandlingsaktiviteter som på grunn av sin art, sitt omfang eller formål krever *regelmessig og systematisk monitorering* i *stor skala* av registrerte

3. *hovedvirksomheten* består av behandling av *sensitive personopplysninger* i *stor skala*, eller personopplysninger knyttet til *straffbare forhold*

Artikkel 37

Personvernombud – intern rolle eller ekstern tjeneste?

- både behandlingsansvarlige og databehandlere er omfattet av regelverket og må utpeke personvernombud

- konsern kan utnevne ett personvernombud og offentlige myndigheter/organ kan utnevne felles ombud
  - må være forsvarlig mht. tilgang til vedkommende, organisasjonsstruktur, størrelse og kompleksitet

- kan etableres som en ekstern tjeneste

Kvalifikasjoner

- **Faglige og formelle kvalifikasjoner**
  - bør stå i forhold til skala og kompleksitet
- **Dybdekunnskap om personvernlovgivning og praksis på området**
  - Kjennskap til sektoren og forståelse av behandlings-aktivitetene, IT-systemer, informasjonssikkerhet mv.
- **Evne til å utføre oppgavene**
  - Personlige kvaliteter og kunnskap
  - Posisjon i virksomheten
  - Personlig integritet og evne til å gjøre etiske vurderinger
  - Evne til å kommunisere og stimulere resten av organisasjonen

Finding that Rare Jack-of-all-trades, the DPO

Artikkel 37

Personvernombudets stilling – virksomheten må sørge for

- **at pvo involveres i spørsmål som gjelder vern av personopplysninger - i rett tid og på riktig måte**
- **at pvo får nødvendige ressurser og tilgang til informasjon og systemer**
- **at pvo får mulighet til å opprettholde dybdekunnskap**
- **at pvo ikke mottar instrukser om utførelsen av oppgaver (avhengig rolle)**
- **pvo skal ikke avsettes eller straffes for utførelsen av oppgaver (stillingsvern)**
- **pvo skal rapportere til høyeste ledelsesnivå**
- **pvo kan ha andre oppgaver, men ikke oppgaver som fører til interessekonflikt**
  - Kan ikke ha stilling som innebærer at ombudet skal bestemme formålet og metode for behandling av personopplysninger

Artikkel 38

Personvernombudet oppgaver

- informere og gi råd til selskapets ledelse og ansatte om forpliktelsene
- kontrollere etterlevelse av personvernregelverket og interne retningslinjer, herunder fordeling av ansvar, opplæring og holdningsskapende tiltak
- gi råd om vurderingen av personvernkonsekvenser (DPIA) og kontrollere gjennomføringen
- være kontaktpunkt for de registrerte
- være kontaktpunkt for- og samarbeide med Datatilsynet
- ha en risikobasert tilnærming til sitt arbeide
- ta behørig hensyn til risikoen forbundet med behandlingsaktivitetene -behandlingens art, omfang, formål og sammenheng

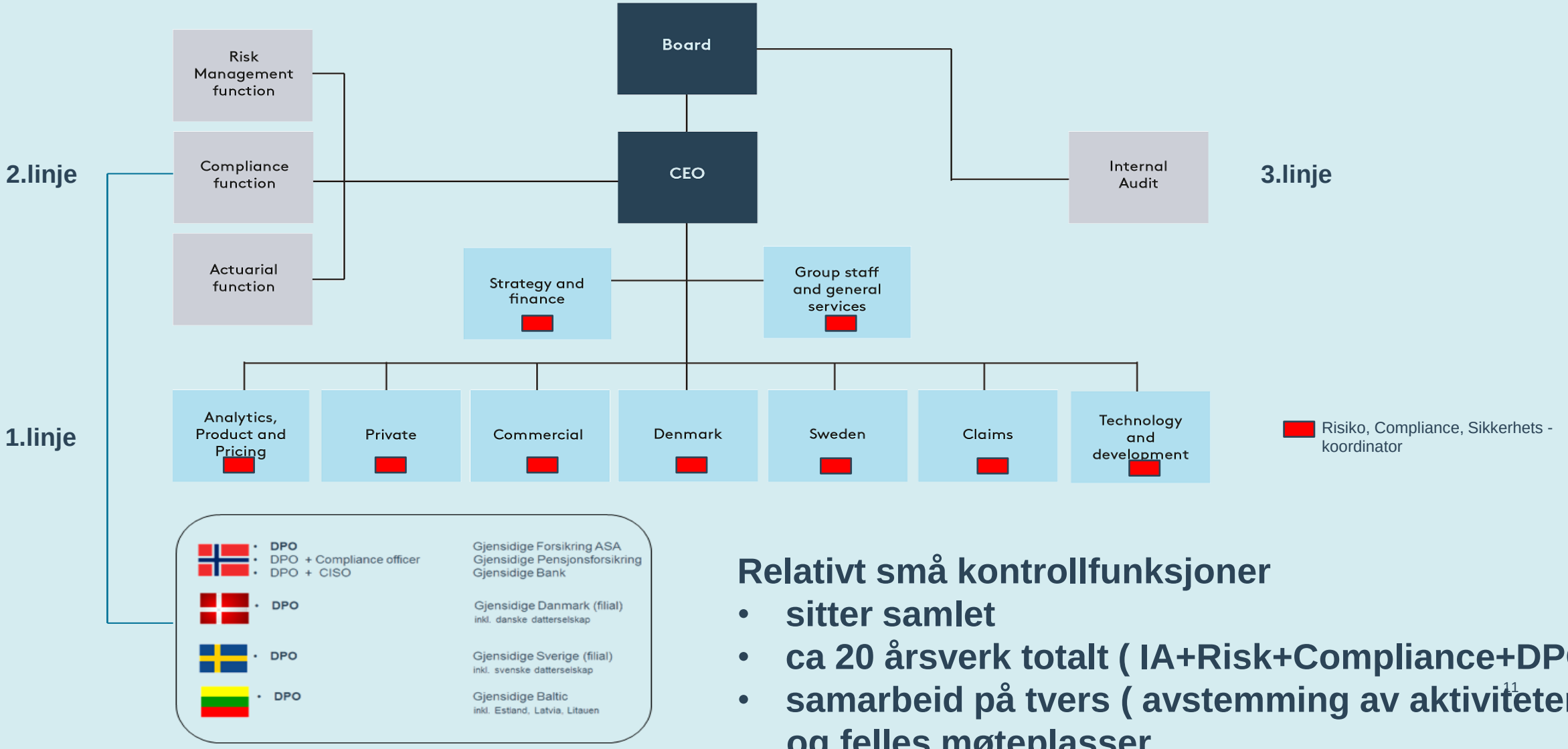
Tasks of the Data Protection Officer

GDPR

En viktig støttende funksjon for å sikre behandlingsansvarliges etterlevelse av kravene i personvernlovgivningen, men PVO overtar ikke behandlingsansvarliges rolle eller ansvar!

Artikkel 39

Kontrollfunksjonene i Gjensidige



Relativt små kontrollfunksjoner

- sitter samlet
- ca 20 årsverk totalt (IA+Risk+Compliance+DPO)
- samarbeid på tvers (avstemming av aktiviteter) og felles møteplasser

GDPR etterlevelse i finansbransjen

Internrevisors rolle
Hvordan kan internrevisjonen bidra?

Samhandling med interne kontrollfunksjoner

Eksempel på samhandling:
Prøvetilsyn

Hvordan kontrollere etterlevelse?

Prøvetilsyn:
Gjensidige Forsikring ASA's behandling av personopplysninger innen privat skadeforsikring i Norge

Konsernrevisjonen i samarbeid med Compliance og DPO

Prøvetilsyn : Formål (scope)

1: Etterlevelse

2: Gjennomføring

Dokumentnavn	Retningslinjer for forberedelse til og gjennomføring av stedlige tilsyn
Hjemmel	Konsernpolicy for Risikostyring og internkontroll
Type	Retningslinje
Gjelder for følgende selskap	Gjensidige Forsikring ASA med datterselskaper
Gjelder for følgende virksomhets-/stabsområder	Alle
Vedtatt av	Styret
Dato vedtatt	19.09.2013
Eier	CRO
Forvalter	CCO
Sist revidert	April 2018
Neste revisjon	April 2019
Versjon	3

Prøvetilsyn : Så realistisk som mulig

Gjensidige Forsikring ASA
Postboks 700 Sentrum
0106 Oslo

Varsel om prøvetilsyn

Konsernrevisjonen ber om at dette varsel behandles som om dette hadde kommet fra Datatilsynet.

Etter at ny personvernforordning trådte i kraft 20.juli 2018 er det ønskelig å foreta prøve tilsyn for å vurdere status for etterlevelse av forordningen.
Det stedlige tilsynet vil finne sted i selskapets lokaler 12.09. fra 0900 – 1500.

Hjemmelsgrunnlag:

Varsel om prøve tilsyn ihht personvernforordningen artikkel 51 av Gjensidige Forsikring ASAs behandling av personopplysninger innen privat skadeforsikring i Norge.

Formål:
Formålet med tilsynet er å vurdere om vesentlige krav i den nye personvernforordningen er implementert for å sikre at personvernet til private kunder i skadeforsikring behandles ihht formål og lovkrav.

Etter avsluttet tilsyn vil Konsernrevisjonen oversende rapporten til styret.

Gjennomføringen av den stedlige kontrollen:
Møtet innledes med en overordnet gjennomgang av virksomhetens behandling av personopplysninger og etablerte styringssystem.

Det er ønskelig at følgende personer er tilstede på møtet, og tilgjengelige under hele kontrollen:

- Den person som har fått delegert myndigheten vedr behandlingen av personopplysninger for private forsikringskunder og vedkommende bør være tilstede i den innledende delen møtet (1. og 2. ihht agenda)
- Den / de som har det daglige ansvaret for behandlingen av personopplysningene
- Den / de som har det daglige ansvaret for utvikling og forvaltning av forsikringssystem og selvbetjeningsløsninger
- Personvernombudet skal være tilstede under hele kontrollen

Den videre gjennomføring av den stedlige kontrollen påvirkes av hva som fremkommer under det innledende møtet. Det kan bli aktuelt å gjennomføre verifikasjoner av ledelsens redegjørelse gjennom samtaler med andre ledere og ansatte, samt innsyn i virksomhetens informasjonssystem og arkiv.

Fra Konsernrevisjonen deltar:

Formelt varsel om stedlig tilsyn med angivelse av

- **Formål**
- **Tidspunkt og sted**
- **Hjemmelsgrunnlag**
- **Gjennomføring og deltakelse**
- **Dokumentasjon og tidsfrister for innsendelse**

Scope:
Behandling av personopplysninger innen privat skadeforsikring i Norge

Prøvetilsyn : Et bredt anlagt tilsyn – mange kontrollpunkter

Kontrollpunkter - etterlevelse

- Art. 5: Grunnleggende prinsipper
- Art. 6.1,f Berettiget interesse som behandlingsgrunnlag
- Art 24 Behandlingsansvarliges ansvar
- Art 25 Innebygd personvern
- Art 30 Protokoller behandlingsaktiviteter
- Art 33&34 Meldeplikter ved brudd
- Art 35 Konsekvensanalyser (DPIA)

Dokumentasjon av hvordan Gjensidige har implementert krav i personvernforordningen i virksomhetens behandling av personopplysninger

- Ansvarlighet ("Accountability")
- Etterlevelse ("Able to demonstrate compliance")

Vi ber om at dokumentasjon som dekker følgende områder oversendes fortløpende og senest innen 31.08.

1. Artikkel 5 – Etablerte prinsipper vedr personopplysninger som bidrar til etterlevelse av personopplysningslov og personvernforordning
2. Artikkel 24 - Tiltak for etterlevelse av prinsipper og krav til personvern; herunder en vurdering av kundeopplevelsen
    a. Foretatte overordnede risikovurderinger vedr personvern
    b. Ledelsens styring og oppfølging personvernkrav
    c. Verktøy og metoder å ha oversikt og kontroll over behandlingen av personopplysninger
3. Artikkel 30 - Protokoll over behandlingsaktiviteter
    a. Protokoll over behandlingsaktivitetene
    b. Oversikt over personopplysninger
    c. Rutiner for å sikre ajouritet
4. Artikkel 35 - Vurdering av personvernkonsekvenser og forhåndsdrøftinger
    a. Metodikk og maler
    b. Kritikalitetsvurderinger og analyser
    c. Prosedyrer for å håndtere personvernkonsekvenser i nye produkter og systemer
        i. Foretatte vurderinger av personvernkonsekvenser
    d. Prosedyrer for forhåndsdrøftinger
        i. Foretatte forhåndsdrøftinger
5. Artikkel 25 - Innebygd personvern og personvern som standardinnstilling
    a. Metodikk og maler
    b. Evalueringer av eksisterende systemer og hvilke gap som ble avdekket
    c. Oversikt / Logg over utviklingsoppgaver
        i. Foretatte evalueringer av de respektive utviklingsoppgavene
6. Artikkel 33 - Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten
    a. Prosedyrer for melding om brudd
    b. Rapporterte hendelser internt
    c. Melding om brudd sendt til Datatilsynet
7. Artikkel 34 - Underretning av den registrerte om brudd på personopplysningssikkerheten
    a. Prosedyrer for registrering av brudd
    b. Rapporterte hendelser internt
    c. Informasjon om brudd sendt til kunden
8. Artikkel 6 (1) (f) - Behandlingens lovlighet
    a. Foretatte vurderinger for de ulike behandlingsaktivitetene
    b. Logg / metode for å ha oversikt over endringer

Prøvetilsyn : Formelt tilsynsmøte med presentasjoner og Q&A

Sak nr.	Tidspunkt	Tema	Presenterer / lead
1.	09:00-09:15	Presentasjon og orientering om prosess for gjennomføring av tilsynet	Konsernrevisjonen
2. a	09:15-10:15	Kort presentasjon av Gjensidiges behandlinger av personopplysninger i saksbehandling, systemer, registre for private kunder innen skadeforsikring	Konserndirektør Privat
2. b		Redegjørelse for hvordan virksomheten har tilrettelagt for å ivareta kravene til behandling av personopplysninger og hvordan dette gjennomføres i den daglige drift	Konserndirektør Privat
3.	10:15-10:45	Presentasjon og demonstrasjon av hvordan protokoll for behandlingsaktiviteter er utformet og holdes ajour	Aktivitetsleder 1
4.	10:45-11:15	Vurdering av personvernkonsekvenser og forhåndsdrøftinger. Presentasjon av metodikk og eksempler på foretatte vurderinger av personvernkonsekvenser respektive eventuelle forhåndsdrøftinger	Aktivitetsleder 1
5.	11:15-11:45	Innebygd personvern og personvern som standardinnstilling. Presentasjon/ demonstrasjon av metodikk og verktøy. Presentasjon av de evalueringer som er foretatt av eksisterende system. Presentasjon av foretatte evalueringer av utviklingsoppgaver.	Aktivitetsleder 2
	11:45-12:30	***Pause***	
6.	12:30-13:00	Håndtering av brudd på personopplysningsikkerheten (artikkel 33 og 34). Presentasjon av rutiner for feil og avvikshåndtering.	Aktivitetsleder 3
7.	13:00-13:45	Foretatte vurderinger for lovlig behandling av personopplysninger	Aktivitetsleder 4
8.	13:45-14:15	Verifikasjoner. Demonstrasjon av et utvalg systemer og verktøy som benyttes i behandlingen av personopplysninger	Aktivitetsleder 5
9.	14:15-14:45	Avslutning	Konserndirektør Privat
		Kort oppsummering. Gjennomgang av hva som bes oversendt etter kontrollen. Informasjon om videre prosess	Konsernrevisjonen

Prøvetilsyn : Formell revisjonsrapport utarbeidet

Grunnlag for Konsernrevisjonens konklusjon:

Intervjuer	Prøvetilsyn og påfølgende samtaler
Dokumentanalyse/ -gjennomgang	Mottatt dokumentasjon før og etter tilsynsdagen
Testing/ Dataanalyser	I / A

Konsernrevisjonens skala for konklusjoner	
	Meget God Etablerte prosesser og kontroller bidrar til måloppnåelse. Det er ikke observert compliancebrudd og risikoen er lav
	Tilfredsstillende Etablerte prosesser og kontroller bidrar i rimelig grad til måloppnåelse. Det er ikke observert vesentlige compliancebrudd eller risikoer
	Mindre tilfredsstillende Prosesser og kontroller har vesentlige svakheter og medfører høy risiko for manglende måloppnåelse, compliancebrudd og/eller tap
	Ikke tilfredsstillende Prosesser og kontroller har kritiske svakheter og medfører risiko utover selskapets risikoappetitt. Tiltak bør følges opp av øverste ledelse i selskapet

Rangering av observasjoner:

1	**Kritisk.** Det er identifisert kritiske svakheter. Forholdet medfører høy risiko og kan true måloppnåelsen på området. Tiltak må iverksettes så snart som mulig.
2	**Viktig.** Det er identifisert vesentlige svakheter. Forholdet reduserer sannsynligheten for måloppnåelse. Tiltak må iverksettes.
3	**Annet.** Det er identifisert forbedringsområder som kan bidra til effektivisering og/eller reduksjon av risiko. Tiltak bør vurderes.

Revisjonsrapport ihht. Konsernrevisjonens metodikk

- Endelig rapport til konsernleder for det reviderte området
- Tilgjengelig for konsernsjef, øvrig konsernledelse samt
- Risikostyring og Compliance
- Totalkonklusjonen inngikk i Konsernrevisjonens kvartalsvise rapport til Konsernstyret

Fokusområder med observasjoner og avtalte tiltak følges opp av Konsernrevisjonen til de er ferdigstilt.

Eksempel på fokusområde, observasjon og tiltak

Fokusområde 3b – Implementering av krav vedr vurdering av personvernkonsekvenser

Tittel			Ansvarlig
Vurdering av personvernkonsekvenser			NN
Observasjon			**Prioritet**
Ihht artikkel 35 – vurdering av personvernkonsekvenser skal det foretas en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. Det er etablert en sjekkliste vedr DPIA foranalyse spørsmål og for gjennomføring av utviklingsprosjekt. Etter gjennomført foranalyse er det etablert regler for om det er nødvendig å gjennomføre en DPIA eller ta kontakt med personvernombud for å be om råd. I det mottatte eksemplet vedr elektronisk pasientjournal ble det svart «JA» på 2 av spørsmålene grunnet økt risiko for at personopplysninger kan komme på avveie. Hvis svaret er «JA» på noen av spørsmålene «må du vurdere å gjennomføre DPIA eller henvende deg til DPO for å be om råd». Vi har ikke mottatt dokumentasjon om hvilken oppfølging som er foretatt.			2
Risiko			
Manglende oppfølging av kommentarer / avvik i utviklingsprosjekter samt dokumentasjon av vurderinger			
Anbefaling	**Ledelsens kommentar**	**Frist**	**Ansvarlig**
3.b.1 Metode for oppfølging av personvernkonsekvenser bør etableres og oppfølgingen bør dokumenteres.	Metode for oppfølging er etablert, men sjekklisten for foranalysen vil utvides slik at oppfølging og konklusjon dokumenteres.	31.12.2018	NN

Prøvetilsyn : Oppsummert

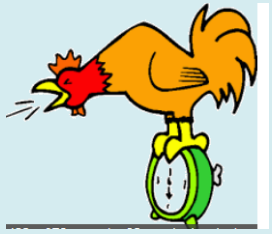
Betydelig læringsverdi

- **Både for behandlingsansvarlig (forretningsområdet) og for Konsernrevisjonen**
- **Åpne og gode diskusjoner**

- **Funn/observasjoner som forventet**
- **Totalt sett en god indikator på nivået av etterlevelse**

Ressurskrevende

- **Mange involverte**
- **Langt tidsrom**
  Oppstartsmøte: 21.08.2018
  Endelig rapportutkast: 15.10.2018



For tidlig og for bredt anlagt?

- **Kort tid etter avslutning av et omfattende GDPR program og 1 måned etter lovens ikrafttredelse**
- **Scopet for tilsynet var bredt (genererte mye arbeid)**

TAKK FOR MEG