Noen aktuelle tema for personvernombud i finans

31.01.2019

SCHJØDT

HVEM I ALLE DAGER SKAL (VIL?) VÆRE PERSONVERNOMBUD?

Uavhengig rolle

Kompetent på – juss – it - sektor

Ikke den som bestemmer eller gir råd om prioriteringer og hvordan PO kan brukes

- Ikke CIO, CTO, HR-direktør – IKKE TVILSOMT ETTER GDPR!
- Internadvokat?
- Compliance-funksjon?
- Ekstern?

Personvernombud

eller

Personvernrådgiver?

Er forskjellen så viktig?

Lov å bruke fornuft?

UAVHENGIGHET

Betydning for plassering i organisasjon og rapporteringsvei

- Kan rapportere til compliance sjef?
- Må ha direkte vei til ledelsen

UAVHENGIGHET – MEN KONTAKT MED LEDELSEN

Hvordan?

Hvor ofte?

Vil endres over tid og kommersielle satsningsområder?

Hvem lytter til hvem?

LEDELSE I PRAKSIS?

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.


MAY THE
FORCE
BE WITH YOU

PERSONVERNOMBUD – KREVES NÅR

Artikkel 37 – krav

DT har kontrollert ombud i offentlig sektor

Nok fokus på nedenforstående?

- Kjerneaktivitet er "systematisk monitorering"
- Profilering anses å være monitorering

PERSONVERNOMBUDET SKAL

- Gi råd om personvern til
  - Ledelsen, resten av virksomheten
  - Bistand til ansatte og henvendelser fra ansatte
  - Henvendelser fra kunder
  - **Undertegne databehandleravtaler?**
  - **Skrive rutiner?**
  - **Bistå i DPIA, men ikke beslutte – hva med ROS-analyser?**

- Overvåke etterlevelse
  - Konflikt ifht å gi råd? Kan «audit» både gi regler og overvåke?

ROS-ANALYSER/RISIKOANALYSE OG DPIA

Under er en illustrasjon av hvordan ROS-analysen er grunnlaget for å ta stilling til om man også å gjøre en DPIA

	Verdi	Risiko	Tiltak
(gammel) ROS 1	Virksomheten	X_{1-3}	Y_{1-4}
(GDPR) ROS 2	☺	X_{4-7}	$Y_{(1-4)+(5-8)}$
Risiko		Liten=OK Stor	↓
DPIA	☺	X_{4-7}	$Y_{(1-8)+(9-12)}$

WP29: PERSONVERNOMBUDET BØR 1/2

- Ha jevnlige møter med øverste ledelse OG mellomledelsen
- Delta i møter der beslutninger om personopplysninger tas – OG ha fått grunnlag for å mene noe om hva man bør beslutte i god tid før møtet
- DPO's (personvernombudet) mening skal tillegges passende vekt
- Om DPOs anbefaling ikke følges, anbefales å dokumentere årsaken til det
- Konsulteres umiddelbart om personvernbrudd har skjedd

WP29: PERSONVERNOMBUDET BØR 2/2

- Få support fra øverste ledelse
- Få tid nok til å utøve jobben
- Få finansielle ressurser nok, andre ressurser nok
- Nødvendig tilgang til HR, IT, legal, security, etc for å skaffe nødvendig input
- Få tilstrekkelig trening
- Ved behov være et team, ikke bare en person

…litt ambisiøst??

LAG ET ÅRSHJUL FOR OMBUDET

Legg inn jevnlige foreteelser

Sett datoer for møter med ledelsen

Særlig fokus på implementering av nye tjenester

Egenkontroll er viktig! (..TBC..)

RUTINE FOR EGENKONTROLL

Formål

Formålet med egenkontroll er å kontrollere om lover og internkontrollrutiner etterleves.

Ansvar

Daglig leder har som behandlingsansvarlig i Selskapet delegert ansvaret for egenkontroll til [tittel på vedkommende som har fått delegert ansvar for egenkontroll/personvernombud]

RUTINE FOR EGENKONTROLL

Egenkontroll

Det er ledelsen ved Selskapet som har ansvar for å gjennomføre egenkontrollen. [Eventuelt kan dette delegeres til personvernombudet.]

Sikkerhetsansvarlig har ansvar for å tilrettelegge gjennomgangen, men skal ikke ha ansvar for gjennomgangen da sikkerhetsansvarlig har medvirket til å spesifisere informasjonssikkerheten.

Selskapet skal gjennomføre egenkontrollen årlig.

Minimum følgende skal kontrolleres:

- At individets rettigheter ivaretas godt nok, se forordningens artikkel 5 og kapittel 3
- At mål som er satt nås og at gjøre korrigerende tiltak foretas ved behov eller avvik samt å følge opp korrigerende tiltak
- Internkontroll
  - Vurdere endringsbehov i eksisterende internkontroll
- Sikkerhetsmål og sikkerhetsstrategi
  - Vurdere behov for endringer i sikkerhetsmål og sikkerhetsstrategi

- Risiko- og sårbarhetsanalyse (risikoanalyse)
  - Vurdere om gjennomførte analyser bør revideres grunnet endrede forhold
- Ved hjelp av stikkprøver skal det kontrolleres at opplysningenes kvalitet er tilstrekkelig i forhold til formålet med behandlingen.
- Alvorlige hendelser og avvik gjennom året skal gjennomgås detaljert
- Mindre avvik kan gjennomgås mer overfladisk.
- Diskusjon bør omfatte årsaker til hendelser og avvik i vid forstand og hvordan hendelser og avvik er håndtert.

Forbedringstiltak skal utarbeides/vurderes og kan gjelde områder som:

- Organisering av sikkerheten
- Partnere og leverandører
- Personell og sikkerhet
- Systemteknisk sikkerhet
- Dokumentsikkerhet
- Beredskap

Avviksskjema, revisjonsrapport

Alle avvik som observeres under egenkontroll, skal registreres på avviksskjema og det skal tas nødvendige skritt for å rette feil og sikre at feil ikke oppstår på nytt.

Avviksskjema skal lagres som en del av Selskapets dokumentasjon av internkontroll for behandling av personopplysninger.

Ved behov skal det etableres egne handlingsplaner for å rette opp systematiske avvik.

Det skal utarbeides en revisjonsrapport som skal drøftes med behandlingsansvarlig.

Man skal ta stiling til eventuelle behov for forbedringer i behandlingen av personopplysninger.

Det finnes langt mer detaljerte sjekklister for de som vil…

AVVIK - BRUDD

Avhengig av faktum, kan brudd på

.. Konfidensialitet, Integritet, Tilgjengelighet

utløse meldeplikt

Hva omfattes - BØR BLI BRANSJESTANDARD

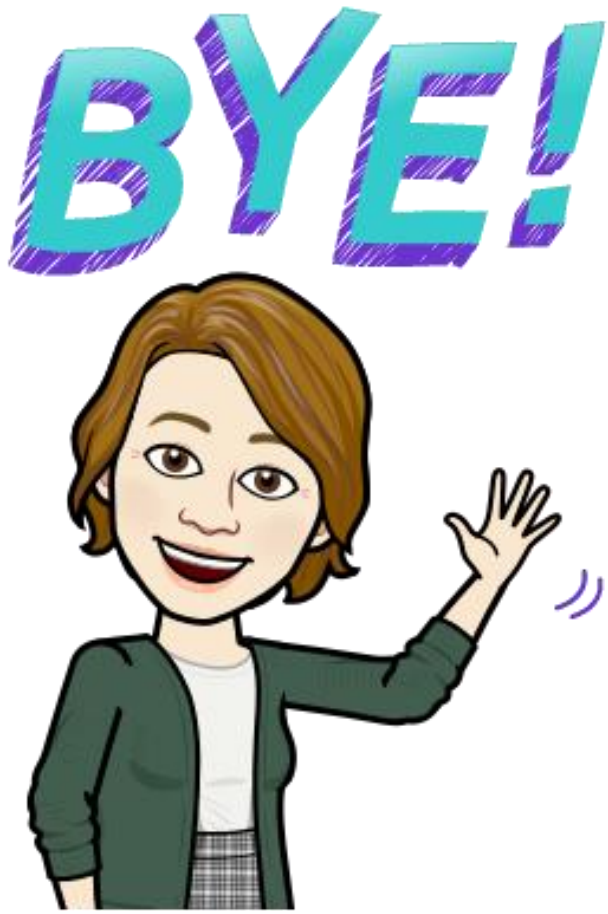
AVVIK - BRUDD

Meldeplikt til DT er «annerledes» enn til individet

Overfor DT kan volum spille en rolle

– for individet gjør det ikke det

Ha rutine for håndtering av brudd


BYE!


USE THE FORCE