BECH-BRUUN

Deloitte.

Rollen som DPO

September 2016

Udpegning af DPO

- Hvilke organisationer (både dataansvarlige og databehandlere) skal have en DPO (artikel 37)?
  - Offentlige myndigheder (undtagen domstole)
  - Private virksomheder, hvis kerneaktivitet består af omfattende databehandling, som kræver regelmæssig og systematisk overvågning af den registrerede i stort omfang
  - Private virksomheder, hvis kerneaktivitet består af behandling i stort omfang af følsomme personoplysninger eller oplysninger om straffedomme og straffelovsovertrædelser
- Koncern kan udpege én fælles DPO – alle etableringer have let adgang til DPO'en
- Flere offentlige myndigheder/organer kan udpege fælles DPO i overensstemmelse med struktur og størrelse
- National ret eller EU-ret (specielle områder) kan fastsætte andre krav til udpegning af DPO
- Øvrige organisationer kan udpege DPO – medlemsstaterne kan lave særregler
- Alle organisationer bør forankre arbejdet med persondata hos en DPO/databeskyttelsesansvarlig

Generelle krav vedr. DPO

- Udpegning på grundlag af faglige kvalifikationer og ekspertise inden for persondatalovgivning og -praksis samt evner til at udføre opgaver oplistet i forordningens artikel 39
- Kan både være medarbejder hos den dataansvarlige og ekstern
- Kontaktoplysninger på DPO'en skal offentliggøres og meddeles til tilsynsmyndigheden
- DPO'en skal tilstrækkeligt og rettidigt inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger
- DPO'en skal støttes i udførelsen af sine opgaver – tilvejebringelse af nødvendige ressourcer til gennemførelse af opgaver, opretholdelse af DPO's ekspertise og adgang til personoplysninger og behandlingsaktiviteter
- DPO'en skal være de registreredes "point of contact" i alle spørgsmål vedr. behandling af deres oplysninger og udøvelse af deres rettigheder i henhold til forordningen

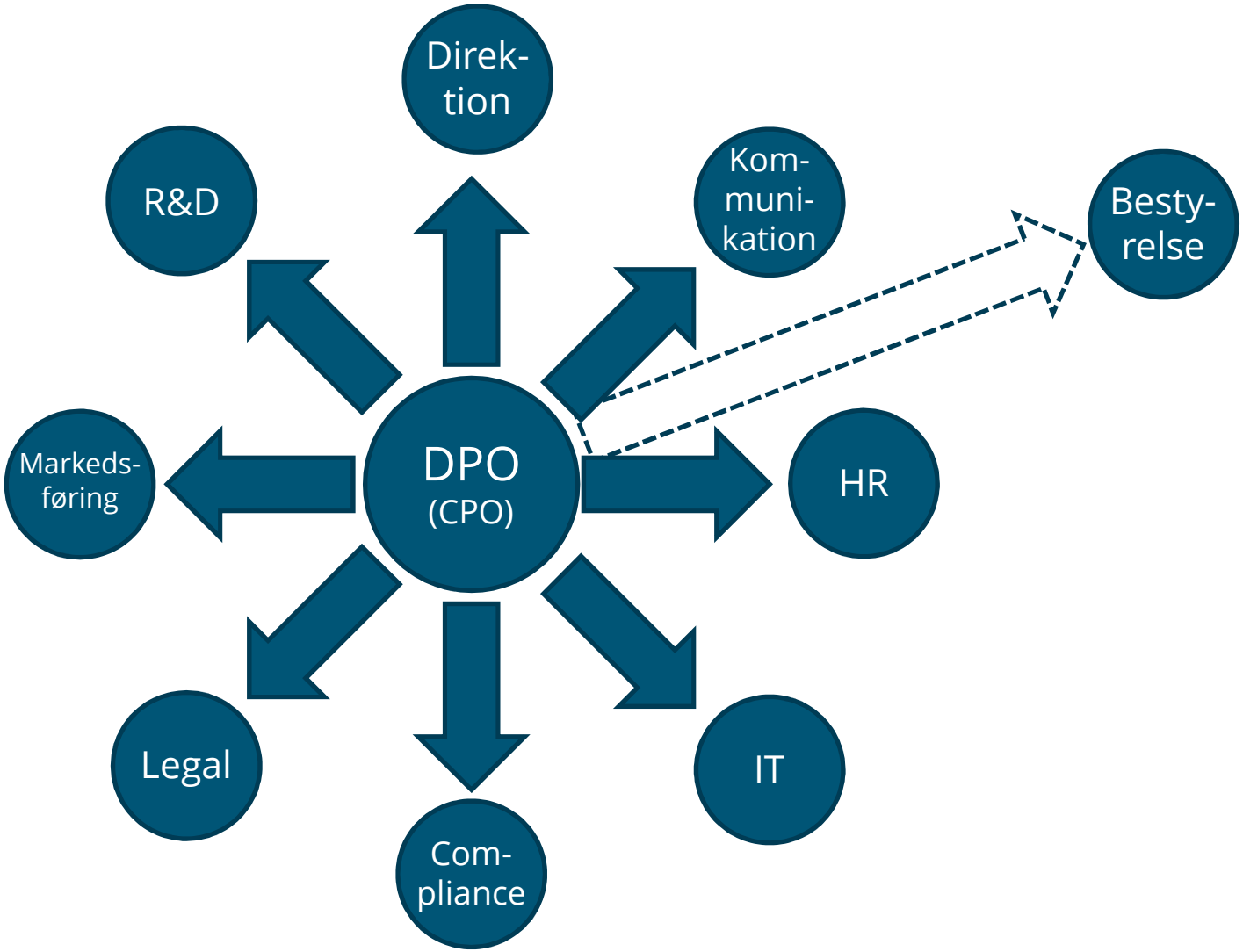
Generelle krav vedr. DPO

- Den dataansvarlige/databehandleren sikre, at DPO'en ikke modtager instrukser vedr. udførelsen af sine opgaver
  - Ikke afskediges eller straffes af dataansvarlig/databehandler for at udføre sine opgaver (ikke en egentlig beskyttet stilling)
  - Rapportere direkte til øverste ledelsesniveau (C-level stilling (CPO))
- DPO'en underlagt tavshedspligt/fortrolighed vedrørende udførelsen af sine opgaver (i overensstemmelse med EU-ret/lovgivningen i en medlemsstat)
- DPO'en kan udføre andre opgaver/pligter – sikre mod interessekonflikt

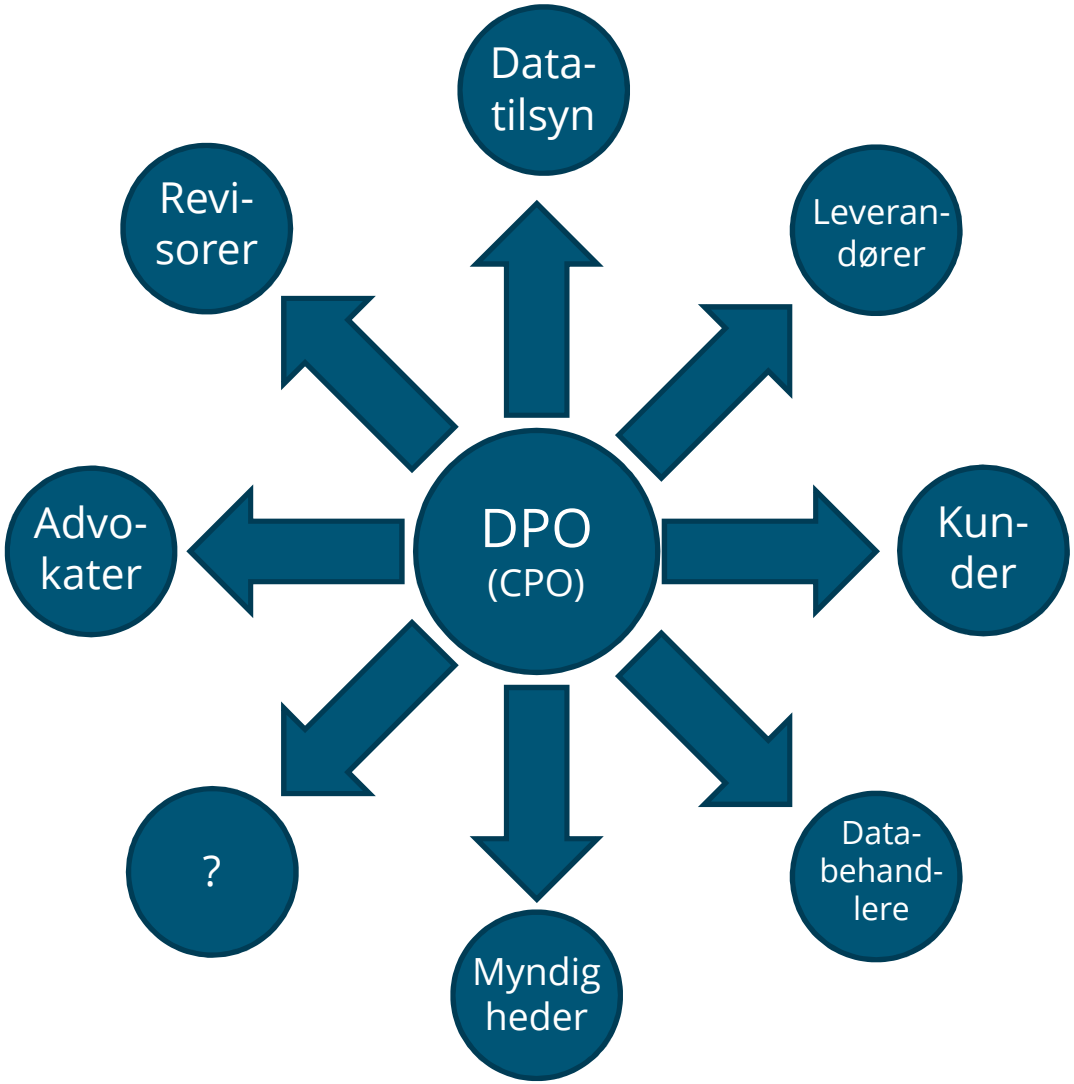
Udpegningen

- Lovkrav i forhold til forretningsbehov
- Interessekonflikter
- Organisationens størrelse/sammensætning
  - Skal det været et egentligt DPO-team?
  - Kritisk størrelse?
  - Privacy-koordinatorer?
- Samarbejde med andre C-level executives (Chief Information Officer CIO, Chief Security Officer CSO, Chief Data Officer CDO Chief Compliance Officer COO CISO (Chief Information Security Officer)
- En organisation med en DPO er ikke automatisk compliant – de materielle krav skal stadig opfyldes

Interne kontaktflader (eksempler)



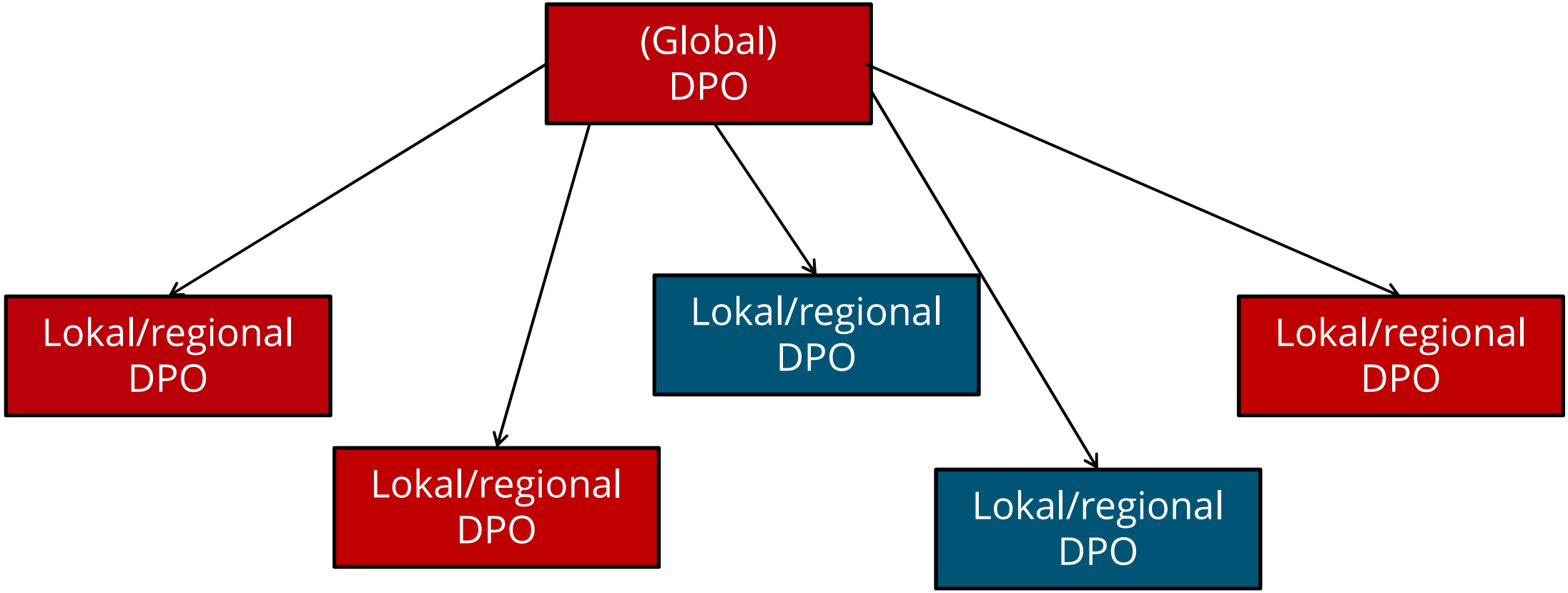
Eksterne kontakter (eksempler)



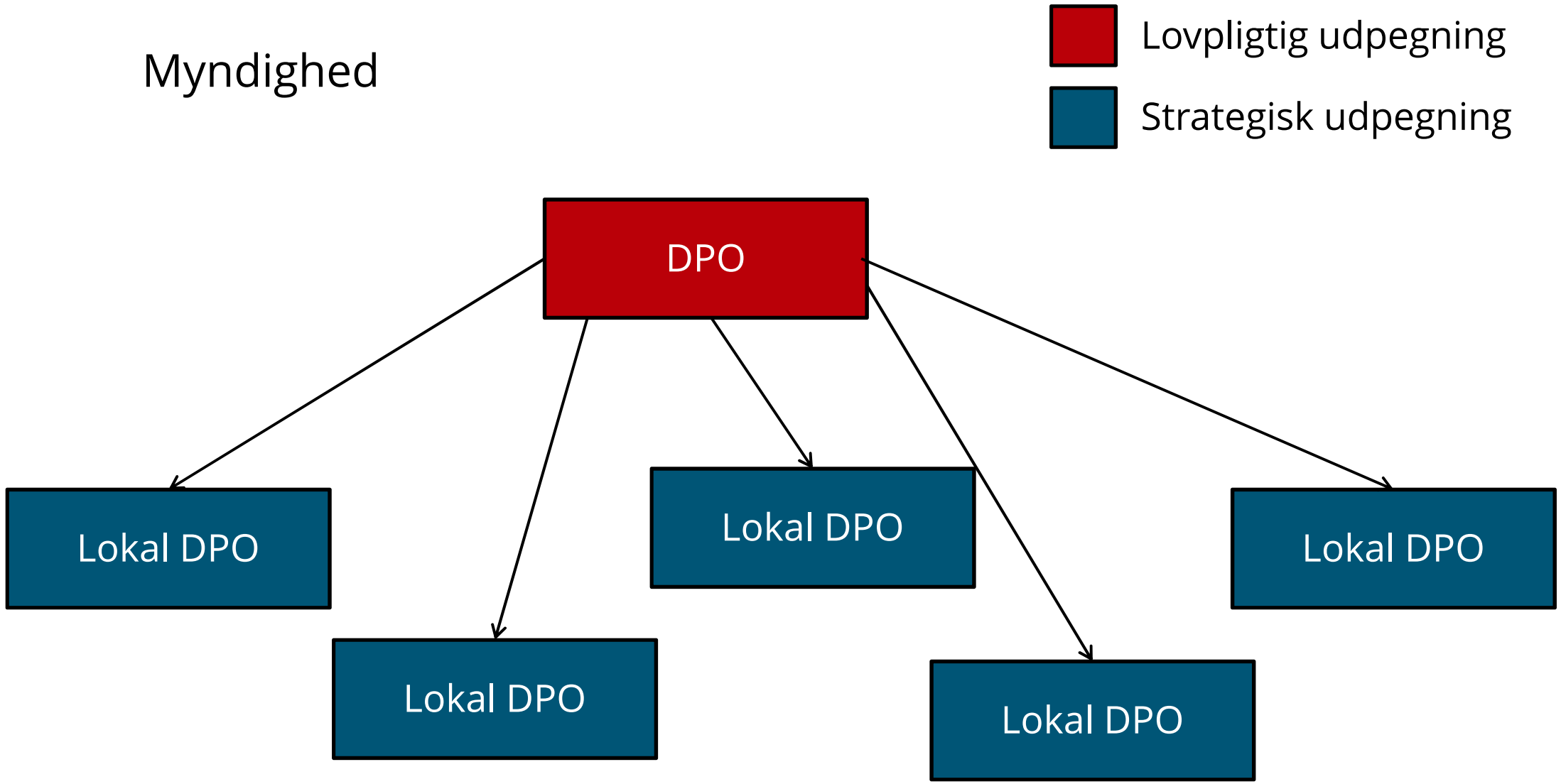
Koncern

Lovpligtig udpegning

Strategisk udpegning



Myndighed


Lovpligtig udpegning
Strategisk udpegning
DPO
Lokal DPO
Lokal DPO
Lokal DPO
Lokal DPO
Lokal DPO

DPO bør have viden om

- Ledelse og organisation
- Viden om tekniske krav til privacy og datasikkerhed
- Konkret viden om den behandling af personoplysninger i den organisation, hvor den pågældende er ansat
- Evnen til at udføre impact assessments, audits, indgå i drøftelser, udarbejde dokumentation og analyser af fx log filer
- Even til at kommunikere effektivt med interne (fra øverste ledelse til piccolinen) og eksterne parter

Forpligtelser og opgaver

- Opretholde balance mellem rollen som selskabets ”trusted advisor” og håndhæver
- Sætte fokus på privacy awareness
- Udarbejde og implementere privacy politikker
- Gennemføre Privacy Impact Assessments
- Overvåge compliance
- Vedligeholde dokumentation
- Administrere hændelser, brud på persondatasikkerheden og underretninger af tilsynsmyndigheden
- Etablere kontakt til tilsynsmyndigheden og interne/interne parter

Administration af politikker

- Implementere politikker og procedurer med henblik på administration af risiko
  - Outsourcing aktiviteter
  - Anvendelse af tredjeparts leverandører (HR, IT, marketing – specielt, hvis de behandler personoplysninger udenfor EU eller i cloudløsninger)
- Opretholde et tæt samarbejde med CISO med henblik på koordinering af compliance og udvikling af information og cyber security politikker og procedurer
- DPO'en bør fokusere på følgende politik-områder:
  - Retningslinjer til direktion, ansatte og ledere
  - Udarbejde retningslinjer til samarbejdsparter og andre tredjeparter som anvender virksomhedens faciliteter og information
  - Samarbejde med HR i forhold til udvikling af politikker, procedurer og processer til behandling af personoplysninger i forbindelse med ansættelse og personaleadministration
  - Samarbejde med IT i forhold til udvikling af politikker, procedurer og processer for informationssikkerhed, håndtering af personoplysninger, outsourcing, BYOD, udvikling af nye løsninger og overvågning af arbejdspladsen
  - Samarbejde med legal og salg/marketing for at sikre compliance med relevant lovgivning og retningslinjer for aftaler, marketing, reklame, profilering og omtale

DPO skal være kendt og respekteret i organisationen

- Regelmæssig ledelsesrapportering på forskellige niveauer
  - Månedligt – status på persondata-compliance i organisationen (sammenhæng med evt. CSR-rapportering)
  - Kvartalsvist
  - Årligt: Egentlig årsrapport om "rigets tilstand"
- Løbende drøftelse med ledelsen om aktuelle forhold
- Politik for underretning af ledelsen om hændelser, sikkerhedsbrud eller lign.
- Single point of contact for nye tiltag i organisationen, som indebærer behandling af personoplysninger

Undervisning/træning

- Vigtig del af persondata og compliance
- Bøder kan også have grundlag i manglende politikker, procedurer og træning
- DPO overordnet ansvarlig for at der gennemføres træning og skabes awareness vedr. politikker og procedurer hos nuværende og nye ansatte, ledelsen og bestyrelsen.
- DPO'en skal deltage i tilrettelæggelse og gennemførelse af træning tilpasset organisationens enkelte afdelinger og teams og sikre opdatering af materiale, når der sker ændringer i lovgivning og retningslinjer.
- Udarbejde en oversigt over undervisningsbehov i forskellige dele af organisationen, fx ud fra en skala fra 0-5 (mulighed for i vis grad at standardisere metoder og materiale)
  - 0: Personalegrupper uden behov for undervisning i persondata (har fx ikke har adgang til personoplysninger i dagligt arbejde).
  - 5: Personalegrupper med stort behov for undervisning i persondata (har fx adgang til store mængder eller meget følsomme personoplysninger i dagligt arbejde)

Etiske standarder for DPO

- Loyalitet
- Kun nødvendig viden
- Fortrolighed
- Interessekonflikter

DPO = multi-talent

- Ændringen i globale privacy frame works og implikationer af brud på persondatasikkerhed medfører, at DPO-rollen får stigende betydning
- DPO'en skal være opmærksom på alle regulatoriske ændringer såvel som ændringer i best practices vedr. informationssikkerhed
- Indsamle oplysninger fra så mange eksterne kilder som muligt via uddannelse og networking
- DPO-rollen kræver mange egenskaber:
  - Forstå og fortolke (anvende) den skiftende lovgivning
  - Kommunikere klart med andre - spec. i fht. lovgivningsmæssige krav, planer, undervise og træne
  - Udarbejde og administrere budgetter
  - Gode skriftlige formuleringsevner
  - Analytisk ift. risiko og GAP
  - Dokumentere og kontrollere processer
  - Være kreativ og forretningsorienteret, når der foreslås løsninger
  - Forstå cyber security risiko og kontroller

Kontakt

Thomas Munk Rasmussen

Partner · København

IP & Technology

T +45 72 27 33 55
M +45 25 26 33 55
E tmr@bechbruun.com