Databeskyttelse i Københavns Kommune

Jesper Andersen / Lone Forsberg

Databeskyttelsesrådgiveren

September 2018

DAGENS EMNER

- Københavns Kommunes anno 2016 & compliancearbejdet
- Governance på databeskyttelsesområdet
- Organisering, ansvar og opgaver - Databeskyttelsesrådgiver
- Kommunens regelheirarki
- DPO Business Partner
- Principper og praktisk samarbejde mellem DPO og DPO Businness Partnerne

NY LOVGIVNING = NYE KRAV OG KONSEKVENSER

Overordnet forskelle ift. persondataloven:

- Den dataansvarlige skal til en hver tid kunne dokumentere sin ansvarlighed, når personoplysninger behandles
- Beskyttelsen af personoplysninger skal ske ud fra en risikobaseret tilgang
- Den dataansvarlige skal udpege og sikre Databeskyttelsesrådgivers mulighed for virke
- Registrerede har meget specifikke rettigheder til at modtage information om de personoplysninger, der behandles om vedkommende, og har i øvrigt direkte adgang til kommunens Databeskyttelsesrådgiver
- Store bøder ved overtrædelser

KOMMUNENS FAKTA PRIMO 2016

600.000+ borgere

Delt administrativ ledelse i 7 forvaltninger

45.000 medarbejdere med ukendt kompetenceniveau ift. håndtering af personoplysninger

Et ukendt antal processer hvor der indgår personoplysninger

Hjemmel baseret på et stort omfang af særlovgivning

Delt governance-struktur på it og data området

Ca. 900 systemer

Stort omfang af databehandlere og dermed behov for databehandleraftaler

Over 50.000 mobile enheder

UDOKUMENTERET COMPLIANCE NIVEAU

KOMMUNENS LEGAL COMPLIANCE PROJEKT

Kommunen etablerer i april 2016 et Legal Compliance Projekt med henblik på:

- At vurdere kommunens compliance niveau ift. Persondataloven
- At vurdere og implementere områder (håndtere GAP's) for at leve op til den nye Databeskyttelsesforordning.

Projektets omfattes 3 spor:

- **Spor 1** – Sikring af dokumentationskrav samt grundlaget for tilrettelæggelse og udmøntning af compliancearbejdet på alle områder I kommunen
- **Spor 2** – Etablering af regler, processer og medarbejderuddannelse, der sikrer håndtering af personoplysninger samt håndtering af registreredes rettigheder
- **Spor 3** – Sikring af governance. Vurdering af sikkerheden I IT porteføljen samt design og implementering af regler, processer og forretningsgange, der sikrer organisatoriske og tekniske foranstaltninger i kommunens it-systemer

GOVERNANCE PÅ DATABESKYTTELSESOMRÅDET

Borgerrepræsentationen

Governance Databeskyttelsesrådgiver

- Revisionsudvalget
- Databeskyttelsesrådgiver
- Databeskyttelsesrådgiver funktionen

Governance Dataansvarlig

- Økonomiudvalget
- Økonomiforvaltningen
- 7 Direktør kredsen
- IT-kreds
- Legal compliance forum
- Business partner forum
- DPO Business Partner (pr. forvaltning)
- Behandlingsprocesansvarlig
- Datastrømsansvarlig

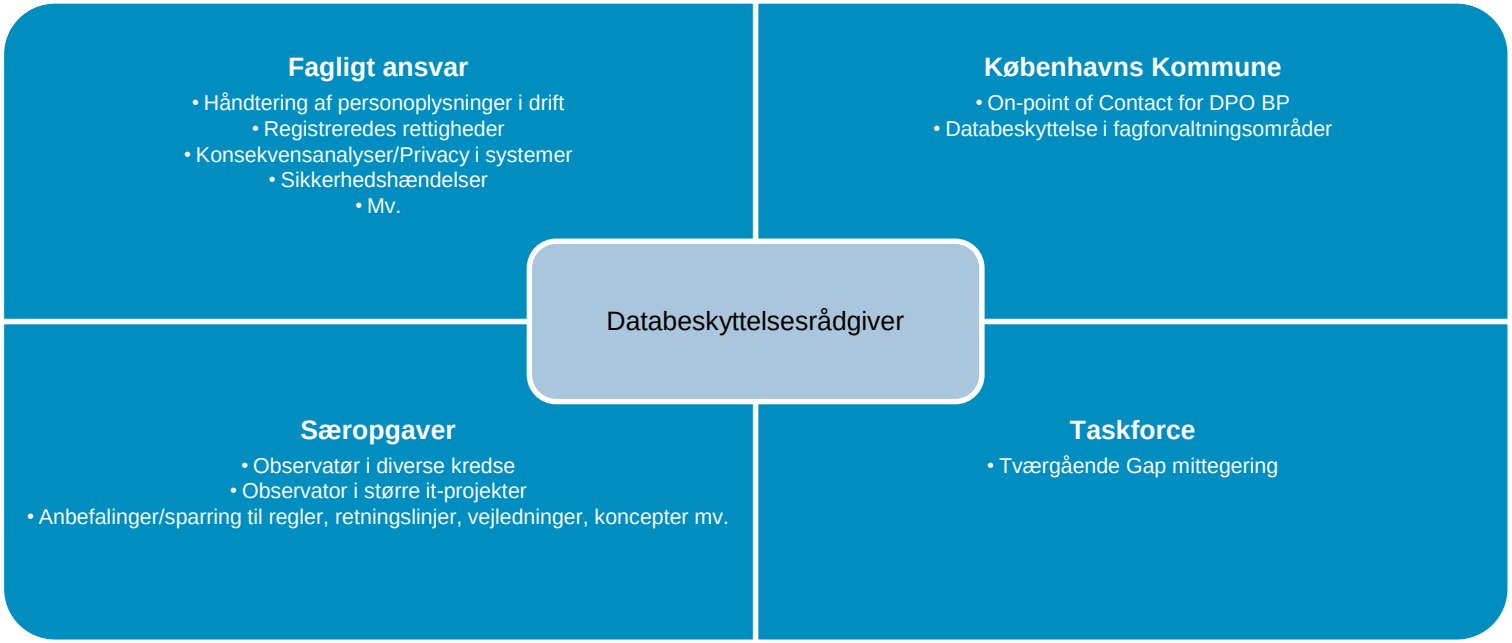
REVISIONSUDVALGETS ANSVAR OG OPGAVER

Ansvarsområder	Opgaver (ikke udtømmende)
Revisionsudvalgets praktiske udmøntning af ansvar og opgaver er fastsat i et revisionsregulativ og Revisionsudvalgets forretningsorden	
At føre tilsyn med Databeskyttelsesrådgivers virksomhed	Revisionsudvalgsmøder 7-8 gange pr. år hvor udvalget orienteres om igangværende og afsluttede aktiviteter hos Databeskyttelsesrådgiver samt om vurdering af compliance i Københavns Kommune. Databeskyttelsesrådgiver har løbende møde med formandskabet Rapportering om særlige forhold eller hændelser Årsrapportering om
At foretage indstillinger til Borgerrepræsentationen om Databeskyttelsesrådgivers rapportering	Databeskyttelsesrådgivers rapportering indstilles til behandling på revisionsudvalgets møder. Når indstilling godkendt oversendes denne til Økonomiforvaltninger, der forud for indstilling til Borgerrepræsentationen indhenter erklæring fra Økonomiudvalget herpå.
At afgive erklæring til Borgerrepræsentationen om indstilling om ansættelse og afskedigelse af Databeskyttelsesrådgiver efter forud indhentet erklæring fra Økonomiudvalget	Er for nærværende ikke nærmere defineret, men vil blive varetaget i samarbejde med Økonomiforvaltningen.

DATABESKYTTELSESRÅDGIVER ORGANISERING

Målsætning med organisering i en matrix model er:

- Sikre og fremme det faglige miljø
- Tydeligt uddelegeret beslutningskompetence
- Ejerskab for helheden – sammenhængskraft
- Godt Socialt fagligt miljø og fælles værdier

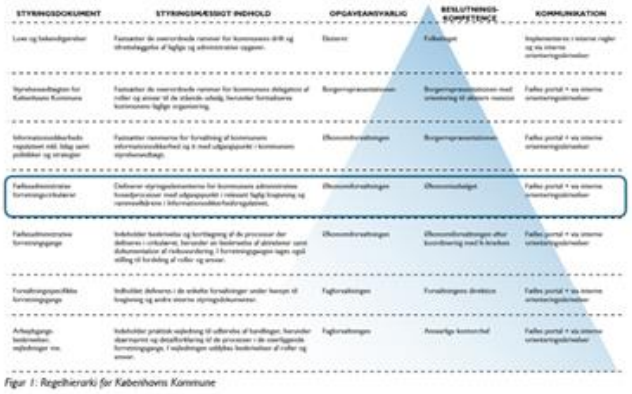


DATABESKYTTELSESRÅDGIVERS ANSVAR /OPGAVER

Ansvarsområder	Opgaver (ikke udtømmende)
Databeskyttelsesrådgiver ansvar og opgaver er fastsat i en funktionsbeskrivelse	
At underrette og rådgive organisationen og de ansatte om databeskyttelse	Scanne og udmelde nyheder – f.eks. retslige afgørelser Rådgivning ifm. forståelsen / fortolkningen / operationalisering af lovgivning Vejledende anbefalinger – fx. uddannelse, registreredes rettigheder etc. Retningsgivende notater – fx. vurdering af slettefrister Møder med DPO Business Partnerne minimum 4 x årligt / pt. hver 2. måned Inddragelse i KK's beslutninger **inden** disse træffes fx ved nye systemer, udstedelse af retningslinjer/processer, etablering af nye behandlingsområder Rådgive borgere
At overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen	Tilsyn på emneområder (20-30 områder svarende til lovgivningens bestemmelser) Tilsyn på enhedsområder (skoler, plejehjem, biblioteker, borgerservicecentre) Tilsyn som følge af kritiske hændelser / observationer / sikkerhedsbrud
At rådgive i forbindelse med udarbejdelse af organisationens konsekvensanalyser	Sikring af at kommunens overholder sin forpligtigelse til at foretage konsekvensanalyse af databeskyttelsen, når en behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder – herunder i forbindelse med nye IT-systemer
At samarbejde med tilsynsmyndigheden.	Høring hos tilsynsmyndigheden ved særlige risikofyldte behandlinger Inddragelse ved klagesager
At fungere som tilsynsmyndighedens kontaktpunkt	Modtage og besvare Datatilsynets henvendelser

KOMMUNENS REGEL HEIRARKI VEDRØRENDE DATABESKYTTELSE & INFORMATIONSSIKKERHED

- Informationssikkerhedspolitik (”ledestjernen” fra topledelsen)
- Informationssikkerhedsregulativ (styringsprincipper og metode beslutningskompetence)
- Cirkulærer rettet mod persondatabeskyttelse og it-beskyttelse og –sikkerhed (regler, roller og ansvar)
  - Persondatabeskyttelse
  - Dokumentation og compliance
  - Organisering af informationssikkerhed
  - IT-beskyttelse og it-sikkerhed
  - It- anskaffelser
  - It- drift og vedligehold
  - It-afvikling og udfasning



Figur 1: Regelhierarki for Københavns Kommune

- Fælles administrative processer og forretningsgange
- Forvaltningsspecifikke processer og forretningsgange

ROLLEN DPO BUSINESS PARTNER

DPO Business Partner

- er kontaktpunkt til Databeskyttelsesrådgiver
- er forvaltningernes (dataansvarlig) vidensperson
- skal til stadighed vurdere complianceniveauet i forvaltningen
- skal rapportere direkte til forvaltningens ledelse om compliance
- skal proaktivt arbejde for, at forvaltningens complianceniveau lever op til lovgivning og regler
- skal rådgive forvaltningens medarbejde.
- skal proaktivt samarbejde og vidensdele med kommunens andre forvaltninger for at sikre tværgående compliance

PRINCIPPER FOR SAMARBEJDET MELLEM DPO BUSINESS PARTNER OG DATABESKYTTELSESRÅDGIVER

- DPO skal sikre adgang til funktionen og dennes rådgivning
- DPO kommer gerne ud eller inviterer til afklarende møder med organisationen
- DPO bekræfter altid skriftligt - anbefalinger / fortolkninger mv. og sikre at DPOBP altid er orienteret om svar på henvendelser
- DPO understøtte med vurderinger/anbefalinger til DPOBP (på anfordring), når denne skal håndterer forvaltningerne i praksis
- DPO sikrer at alle involverede parter afstemmer aktiviteter (tilsyn, overvågning, gap mittegering), så disse er dækkende for KK
- DPO sikre fællesskab / videndeling ved Business Partner Forum

- DPOBP har selv en aktiv rolle for at bringe forhold til drøftelse i forum eller overfor DPO direkte
- DPOBP, skal sikre at forvaltningen som dataansvarlig selv træffe beslutninger, fører ledelsestilsyn og kan gøres ansvarlige for håndtering og beskyttelse af personoplysninger fx gennem dokumentation, skriftlige vurderinger mv.
- DPOBP skal sikre formidlingen til forvaltningerne på beslutninger /anbefalinger og henstillinger
- DPOBP skal sikre at DPO inddrages som lovgivningen foreskriver.

SAMARBEJDET DPO / DATAANSVARLIGE (DPOBP)

Eksempel på praktisk samarbejde
Løbende (daglige) driftsspørgsmål fra DPOBP, brug af samtykke, billeder på sociale medier, anvendelse af hjemmelsgrundlag jf. særlov
Tværgående rådgivning, fx. tv-overvågning, statistisk arbejde, SoMe håndtering
Principielle forhold, hvor DPO kan se at kommunen har behov for hjælp til fortolkning eller fælles principper / metoder for at håndtere personoplysninger fx. Metode for vurdering af slettefrister eller konsekvensanalyser.
Inddragelse ved ændringer i processer, så disse risikovurderes / konsekvensanalyseres og hvordan oplysninger skal registreres for at overholde dokumentationskrav.
Rådgivning / inddragelse ved sikring af compliance af eksisterende/nye behandlingsprocesområder, ny digitaliseringstiltag, eksisterende og nye systemer
Rådgivning mhp. at understøtte DPOBP kan videregive dette til organisationen – fx. uddannelse
Sikkerhedsbrud, hvor vi rådgiver ifm. vurdering hændelserne herunder anmeldelse til Datatilsynet/underretning til registrerede
Tilsynsaktiviteter, hvor der er størst behov / størst risici / afstemt med andre complianceaktiviteter
Gap håndtering / taskforce / opfølgning på complianceaktiviteter – sker gennem mere traditionel projektledelse / koordineringsarbejde i tæt samarbejde med DPOBP