Vejledning om roller og ansvar for compliance og informationssikkerhed

Organisation	**Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)**
Dokument navn	Roller og ansvar for GDPR compliance og informationssikkerhed v. 1.0 docx
Dokument ejer	Daniel Bach og Michael Drews Olsen
Senest ændret	04 december 2018
Autoriseret af	
ISO 27002	6.1.1 - Definere og fordele alle ansvarsområder for informationssikkerhed
GDPR-reference	Artikel 24.1 – Gennemføre passende organisatoriske foranstaltninger
Dataklassifikation	Internt dokument

Version nr.	Dato	Revisions forfatter	Beskrivelse
1.0	04 december 2018	Daniel Bach, Michael Drews Olsen	Første version

Formål:
Det er en forudsætning for at komme i mål med compliance og informationssikkerhed i kommunen, at roller og ansvar er defineret og placeret i organisationen.

Det er denne vejlednings formål at hjælpe kommunerne i DSD, som er tilsluttet den fælles databeskyttelsesfunktion, i forhold til definition af roller og ansvar med henblik på implementering og udførelse af opgaver vedrørende compliance og informationssikkerhed.

I vejledningen findes der *eksempler* på organisering, roller og ansvar i relation til compliance og informationssikkerhed.

Omfang: Alle kommuner i DSD tilsluttet den fælles databeskyttelsesrådgiverfunktion.

Anbefaling
Kommunens direktion bør sikre, at organisatoriske foranstaltninger, deriblandt roller og ansvar for sikkerhed og compliance, er defineret og implementeret i hele den kommunale organisation. Således kan kommunen sikre og påvise, at alle medarbejdere og ledere er bevidste om deres ansvar i forhold til efterlevelse af kravene i persondataforordningen, databeskyttelsesloven samt kommunens informationssikkerhedspolitikker.

Sikkerhedsansvarlig
Kommunaldirektøren er den øverste ansvarlige for compliance og informationssikkerhed i kommunen. Kommunaldirektøren varetager typisk rollen som sikkerhedsansvarlig, men det er muligt at udpege andre i kommunen som sikkerhedsansvarlig. Det kan f.eks. være en forvaltningsdirektør eller en it- eller digitaliseringssikkerhedschef i kommunen.

Den sikkerhedsansvarlige påser, at informationssikkerhedspolitikken afspejler og understøtter kommunens mål og visioner og lever op til de ønskede mål.

Den sikkerhedsansvarlige har det overordnede ansvar for informationssikkerheden og sætter den strategiske retning og prioritering - risikovilligheden. Har overblik over risici. Fordeler og placerer roller og ansvar i organisationen. Sikrer, at arbejdet med informationssikkerhed har andre lederes opbakning. Sikrer, at de resurser, der er nødvendige for informationssikkerhed og compliance, er tilgængelige i organisationen.

Styregruppen for informationssikkerhed
Udvalget er tværorganisatorisk, typisk med den sikkerhedsansvarlige som formand.

Styregruppen for informationssikkerhed består typisk af kommunaldirektøren, forvaltningsdirektører, sikkerhedsansvarlig, HR-chef, IT-chef, sikkerhedskoordinator, databeskyttelsesrådgiveren. Styregruppen holder regelmæssige møder vedrørende informationssikkerhed og compliance.

Styregruppen fastsætter det overordnede sikkerhedsniveau og definerer det tilhørende informationssikkerhed og compliance program. Sikrer, at programmet samt informationssikkerhedspolitikken implementeres og vedligeholdes hensigtsmæssigt og effektivt. Behandler det overordnede risikobillede for informationssikkerhed, og sikrer at uacceptable risici håndteres. Sikrer, at det besluttede sikkerhedsniveau udmøntes i budgetter og indgår i relevante handlingsplaner.
Databeskyttelsesrådgiverens deltagelse er hovedsagelig i rollen som observatør, men kan bidrage med retningslinjer og fortolkning af lovmæssige krav.

Sikkerhedskoordinator
Sikkerhedskoordinatoren varetager rollen som kommunens primære koordinator for informationssikkerhed og compliance og rapporterer til kommunens sikkerhedsansvarlige.

Sikkerhedskoordinatoren arbejder med at sikre, at compliance og informationssikkerhed udbredes og implementeres i alle fagcentre/forvaltninger (herefter fagcentre), primært igennem samarbejde med de faglige sikkerhedskoordinatorer.

Sikkerhedskoordinatoren er den primære kontaktperson til databeskyttelsesrådgiveren og deltager sammen med sikkerhedskoordinatorerne fra andre DSD-kommuner i regelmæssige møder med henblik på at harmonisere tilgangen til arbejdet med compliance- og informationssikkerhed.

Fagansvarlig, centerleder

Den fagansvarlige har ledelsesansvaret for et område eller et fagcenter i kommunen. En fagansvarlig har det overordnende ledelsesansvar for efterlevelse af sikkerhedspolitikker, retningslinjer, complianceopgaver og andre databeskyttelsesretlige pligter inden for det pågældende fagcenter. Den fagansvarlige har eventuelt ejerskab af understøttende systemer og/eller leverandører, med dertilhørende ansvarsopgaver.

Den fagansvarlige udpeger en faglig sikkerhedskoordinator, der i samarbejde med kommunens sikkerhedskoordinator og databeskyttelsesrådgiver arbejder på at sikre fagcentrets compliance og informationssikkerhed.

Faglig sikkerhedskoordinator

I hvert fagcenter er der blandt afdelingsledere udpeget en faglig sikkerhedskoordinator, som er den fagansvarliges højre hånd i forhold til arbejdet med compliance og informationssikkerhed.

Fagcenterets faglige sikkerhedskoordinator varetager den overordnede styring af informationssikkerheden i fagcenteret og varetager sikkerhedsopgaven/rollen ved siden af de andre opgaver, som koordinatoren har. I større fagcentre kan der med fordel udpeges en specialiseret medarbejder (herefter compliance ambassadør) som støtter den faglige sikkerhedskoordinator. Dette kan eksempelvis være en sikkerhedsadministrator, som udfører daglige brugeradministrative opgaver.

Den faglige sikkerhedskoordinator har et tæt samarbejde med kommunens sikkerhedskoordinator samt fagcentrets compliance ambassadør.

Compliance ambassadør

Compliance ambassadører bør udpeges i større fagcentre, hvor der findes mange komplekse behandlingsaktiviteter. En compliance ambassadør sikrer, at løbende obligatoriske compliance- og informationssikkerhedsopgaver udføres. Det vil være en fordel, hvis compliance ambassadøren besidder tekniske og/eller juridiske færdigheder.

Eksempler på opgaver for en compliance ambassadør:
Bistår med kortlægning og vedligeholdelse af behandlingsaktiviteter, sikrer at registreredes rettigheder efterleves, ajourfører oplysningssedlen, rapporterer ændringer eller nye behandlingsprocesser, sikrer vedligeholdelse af brugeradgang, påser at databehandleraftalen er gyldig og tilsynet er udført efter planen, sikrer medarbejderes bevidsthed omkring compliance og informationssikkerhed (awareness), udbreder kendskab til politikker og retningslinjer samt sikrer, at procedurer for sikkerhedshændelser er fulgt (se også DSD vejledningen om compliance årshjul).

Ejere af systemer og data

Systemer - og/eller data, ejes typisk af den fagansvarlige eller en chef, der har fået delegeret ansvaret. Ofte er der sammenfald mellem system og dataejerskab, men et system kan godt have flere dataejere.

Ejeren fastlægger, hvem der må få adgang til systemer og/eller data, under hvilke betingelser system og/eller data må anvendes, og hvordan system og/eller data skal beskyttes.
En systemejer kan eje et eller flere systemer. Endelig har ejere også ansvaret for eksterne parter, der udfører udvikling, drift og vedligeholdelse af systemet.

Den fagansvarlige kan udpege en eller flere administratorer som varetager de daglige og praktiske opgaver for systemets drift, relation til leverandør.

Databeskyttelsesrådgiver

Databeskyttelsesrådgiveren rapporterer til den øverste ledelse i kommunen og i sidste instans til kommunalbestyrelsen. Rådgiveren er en uafhængig funktion, og må ikke som led i sin funktion modtage instruks om, hvordan DPO-opgaverne skal udføres.

Databeskyttelsesrådgiverens funktion er at understøtte, at kommunen overholder reglerne i databeskyttelsesforordningen, herunder at underrette og rådgive organisationen og de ansatte om databeskyttelse samt føre tilsyn med kommunens overholdelse af regler vedrørende databeskyttelse.
Det er hensigtsmæssigt at databeskyttelsesrådgiveren deltager i møder med styregruppen for informationssikkerhed, for blandt andet at drøfte compliance udfordringer samt lovmæssige krav.

It-chef

Varetager rollen for IT-drift, anskaffelse, opsætning og teknisk sikkerhed af kommunens infrastruktur. IT-chefen kan udpeges som dataansvarlig for tværorganisatoriske systemer såsom e-mail.

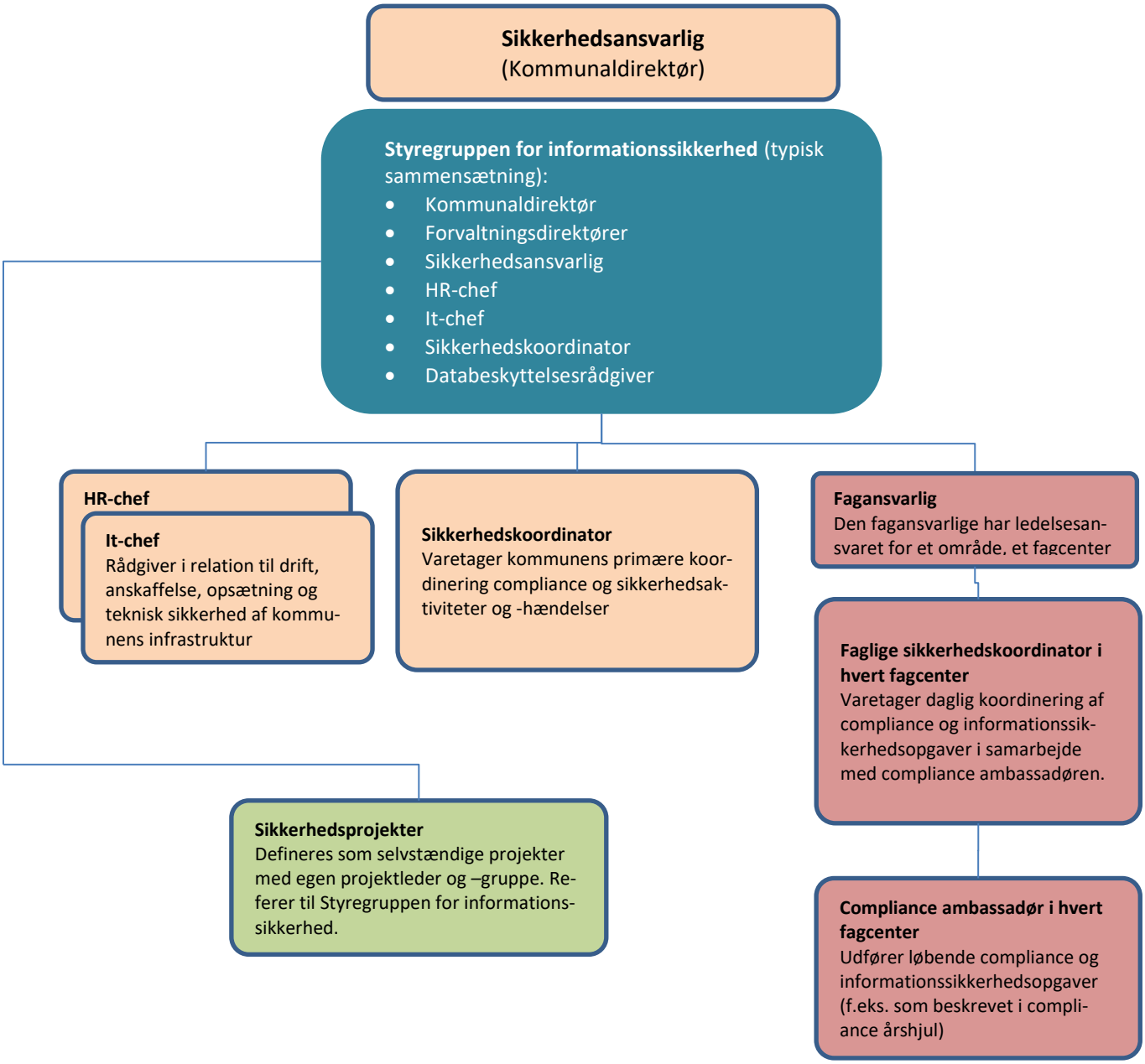
HR-chef

HR-chefen har ansvaret for personalerelaterede sager, herunder personalepolitik og håndbog, intern uddannelse, lederuddannelsen og konsulentbistand til forvaltninger. Personaleafdelingen har ansvaret for at sikre at rammerne for ansættelsesmæssige forhold er beskrevet og kommunikeret. Det er de respektive lederes ansvar at sikre, at det efterleves. Bidragsyder til bevidsthedsskabende kampagner om informationssikkerhed (awareness) sammen med styregruppen for informationssikkerhed.

Sikkerhedsprojekter

Defineres som selvstændige projekter med egen projektleder og gruppe. Referer til styregruppen for informationssikkerhed.

Organisations diagram for compliance og informationssikkerhed



Bilag A (standardinformation i vejledninger fra databeskyttelsesrådgiverfunktionen i DSD)

Relevante definitioner:

»dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. I DSD-kommuner kalder vi denne rolle for [Fagansvarlig].

»fagansvarlig«: en fagansvarlig har ledelsesansvaret for et område, et center, eller en forvaltning i kommunen. En fagansvarlig har det overordnende ledelsesansvar for behandlingsaktiviteter (behandlingen af personoplysninger) inden for det pågældende område, center eller forvaltning. En fagansvarlig refererer til den administrative direktion i kommunen.

»databehandler«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne

»fagcentre«: en Kommune er opdelt i forskellige enheder med fokus på et specifikt pligtområde. Disse enheder kaldes også fagcentre, afdelinger, forvaltninger eller centre. Et fagcenter har en eller flere [fagansvarlig], der bærer rollen som dataansvarlige.

Officielle kilder:

Datatilsynet:
Persondataforordningen:
Databeskyttelsesloven: