13-02-2020

Kommissorium for organisering af Databeskyttelse (GDPR) i Ishøj Kommune

Baggrund

Den 25. maj 2018 trådte EU's databeskyttelsesforordning (GDPR) som bekendt i kraft. I den forbindelse valgte Ishøj Kommune at nedsætte en central task force, en udvidet task force (task force +) med deltagelse af alle centre samt en central informationssikkerhedsgruppe, som har haft til opgave at understøtte organisationen i implementeringen og efterlevelsen af kravene i GDPR.

Henover sommeren 2019 har vores Databeskyttelsesrådgiver, Daniel Bach, foretaget en modenhedsmåling på alle driftssteder og 'enheder' (niveau 3) i Ishøj Kommune for at afdække, hvor langt vi er nået i forhold til overholdelse af kravene i GDPR (compliance). På baggrund af resultaterne har Daniel Bach udarbejdet en rapport over Ishøj Kommunes modenhedsniveau, som er fremlagt for Koncernledelsen i december 2019.

Resultaterne fra modenhedsmålingen peger i retning af, at der er store forskelle i modenhedsniveauet i organisationen, hvilket kan tyde på, at den nuværende organisering ikke fungerer optimalt. Der er ligeledes områder, hvor Ishøj Kommune ikke lever op til kravene i GDPR. Konklusionen i rapporten er således, at Ishøj Kommune skal hæve vores compliance niveau generelt.

Herudover peger modenhedsmålingen på, at der er utilstrækkelige ressourcer i Ishøj Kommune til arbejdet omkring overholdelse af GDPR og databeskyttelsesloven.

På denne baggrund er informationssikkerhedsgruppen blevet bedt om at revurdere den nuværende organisering omkring GDPR og komme med et kommissorium for en fremtidig organisering.

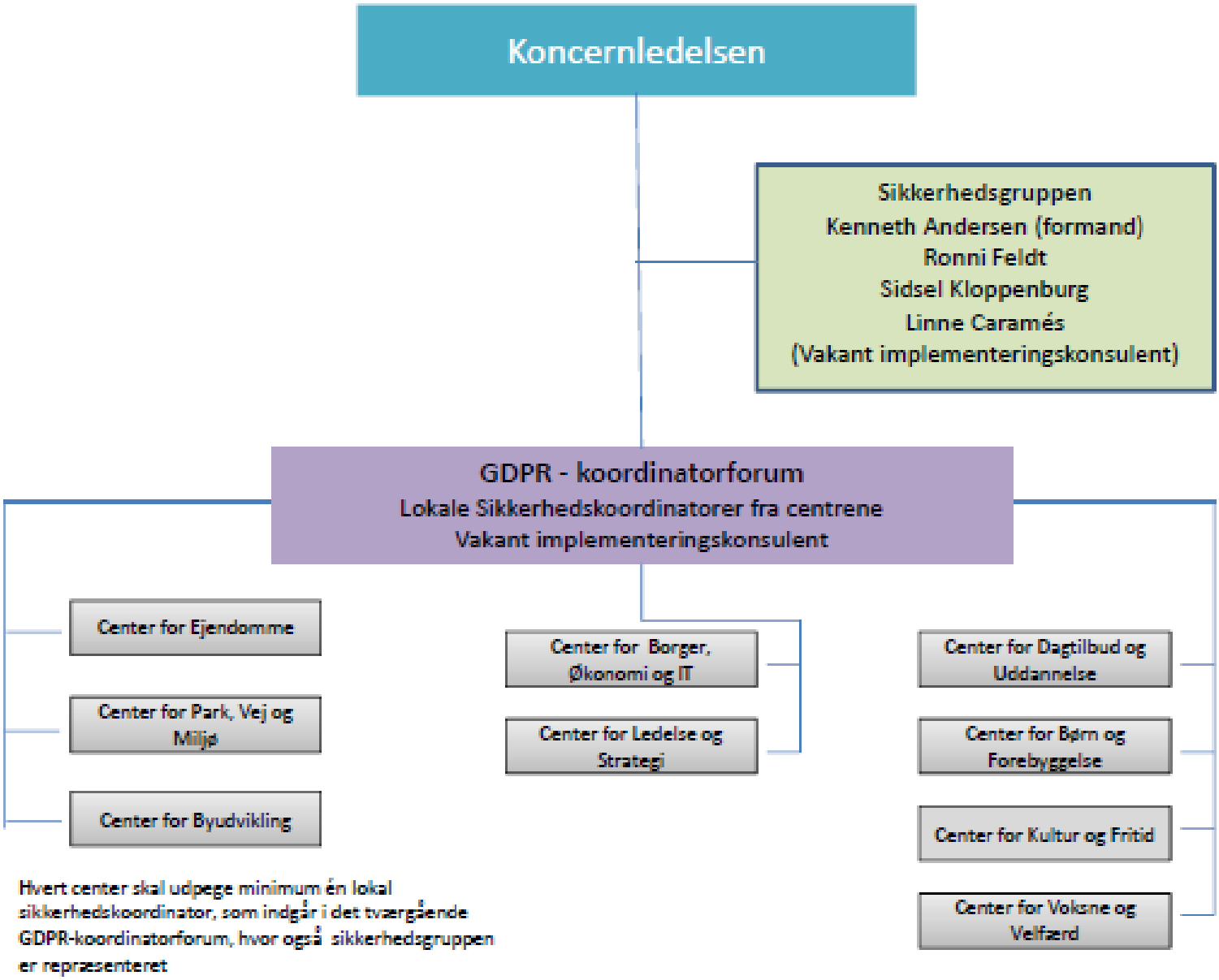
Formål

Formålet med den nye organisering er at sikre:

- at det generelle modenhedsniveau omkring GDPR og informationssikkerhed højnes i hele organisationen.
- at kravene i GDPR efterleves og når ud til de yderste led i organisationen.
- at ressourcerne i organisationen bruges mest hensigtsmæssigt.

I nedenstående vises et forslag til den fremtidige organisering.

Organisering af GDPR i Ishøj Kommune



Hvert center skal udpege minimum én lokal sikkerhedskoordinator, som indgår i det tværgående GDPR-koordinatorforum, hvor også sikkerhedsgruppen er repræsenteret

Den nye organisering
Der skal som i dag være en central sikkerhedsgruppe, som drøfter og koordinerer den overordnede og strategiske indsats vedrørende GDPR og informationssikkerhed i Ishøj Kommune. Ud over GDPR forventes der at komme yderligere it- og datasikkerhedsmæssige krav og standarder, herunder ISO og NSIS[1], hvor der ligeledes bør ske en koordinering af indsatser og tiltag.

For at få GDPR implementeret i hele organisationen, skal der være en organisering, hvor centrene er repræsenteret via lokale sikkerhedskoordinatorer. De lokale sikkerhedskoordinatorer (GDPR-superbrugere) skal opkvalificeres og tildeles et mere formaliseret ansvar for datasikkerhed, end de har i dag. I den forbindelse er tanken, at vi indkøber et fælles uddannelsesforløb for de lokale sikkerhedskoordinatorer, så de bliver klædt på til at løfte opgaven i fællesskab. Det er derfor vigtigt, at hvert center peger på minimum én lokal sikkerhedskoordinator, som interesserer sig for GDPR, og som ønsker et kompetenceløft på området.

Roller og ansvar i organiseringen
Det overordnede ansvar for Ishøj Kommunes informationssikkerhed og compliance følger ledelsesstrukturen.

Sikkerhedsgruppen
Den overordnede sikkerhedsgruppe skal koordinere den strategiske indsats vedrørende GDPR og informationssikkerhed i Ishøj Kommune.

Gruppens opgaver vil primært bestå i:

- Håndtering af overordnede risikoforhold, herunder eskalation til de forskellige ledelsesniveauer
- Oplæg til prioritering af strategiske indsatsområder i relation til GDPR
- Håndtering af komplicerede sikkerhedshændelser
- Udarbejdelse af de tværgående procedurer og skabeloner omkring informationssikkerhed
- Sparring med de lokale sikkerhedskoordinatorer
- Oplæg til Direktion, KCL og det politiske niveau omkring GDPR

Lokale sikkerhedskoordinatorer
Der skal udpeges minimum én sikkerhedskoordinator i alle centre, som skal opkvalificeres til 'superbrugere' inden for GDPR. Koordinatorerne deltager i GDPR-koordinatorforum, hvor også sikkerhedsgruppen er repræsenteret.
De lokale sikkerhedskoordinatorer fungerer som bindeleddet mellem den overordnede sikkerhedsgruppe og centrene. Sikkerhedskoordinatorenes rolle bliver derved at:

- deltage i uddannelse og holde sig opdateret omkring GDPR
- sørge for, at informationer, instrukser, procedurer mv. fra sikkerhedsgruppen formidles og implementeres i eget center
- facilitere og koordinere overholdelse af kravene i GDPR i eget center, herunder krav vedr. dokumentation og kontrol
- håndtere simple sikkerhedsbrud samt indberetning og dokumentation efter anvisninger fra sikkerhedsgruppen
- sparre med og rådgive de øvrige ansatte i ens center omkring GDPR
- eskalere komplekse 'sager' og hændelser til sikkerhedsgruppen

[1] ISO henviser til forskellige internationale standarder for håndtering af informationssikkerhed.
NSIS (National Standard for Identiteters Sikringsniveauer) er en standard for entydig identifikation af en fysisk person

For at de lokale sikkerhedskoordinatorer kan lykkes med disse opgaver, er det en forudsætning, at de har den nødvendige tid og det nødvendige mandat fra ledelsen. Centercheferne beslutter hvordan arbejdet med GDPR organiseres internt i deres center.
Det anbefales, at der ansættes en implementeringskonsulent i en tidsbegrænset stilling (1-2 år), som indgår i GDPR-koordinatorforum og eventuelt også i sikkerhedsgruppen afhængig af profil. Implementeringskonsulenten skal understøtte GDPR-arbejdet, der hvor KCL efter indstilling fra sikkerhedsgruppen vurderer, at behovet er størst. Forslag til stillingsbeskrivelse findes i bilag 1.

Opkvalificering af de lokale sikkerhedskoordinatorer
De lokale sikkerhedskoordinatorer tildeles større ansvar og flere konkrete opgaver med den nye organisering. Det er derfor vigtigt, at de får den rette uddannelse, så de alle bliver klædt på til at løfte denne opgave.

Vi foreslår, at vi indkøber et firmakursus skræddersyet til vores behov via eksempelvis COK. Herved sikrer vi, at alle de lokale sikkerhedskoordinatorer får samme viden og samme sprog omkring GDPR, hvilket gør det lettere for dem at sparre med hinanden, med medlemmerne af sikkerhedsgruppen og med kommunens databeskyttelsesrådgiver.

Kurset skal bl.a. have fokus på følgende emner:

- En grundlæggende introduktion til GDPR samt de krav, der ligger heri.
- En forståelse af, hvordan GDPR skal indtænkes i den kommunale virkelighed. GDPR rummer f.eks. i særlige tilfælde en mulighed for at sætte hensynet til borgeren højere end efterlevelse af lovgivningen. Herudover er det vigtigt at have for øje, at kommunen også skal efterleve en lang række andre love, herunder forvaltningsloven og en række særlovgivninger, som har forrang for GDPR.
- De registreredes rettigheder. Hvilke rettigheder har borgerne efter GDPR.
- Krav til samtykke, oplysningspligt, dokumentation, kontrol mv.
- Introduktion til risikovurdering og konsekvensanalyse
- Relevante afgørelser og fortolkninger på området.

Formålet med kurset er at sikre, at de lokale sikkerhedskoordinatorer har en solid forståelse for indholdet i GDPR og herved er i stand til at sikre, at deres respektive center efterlever reglerne.

Evaluering
Den nye organisering evalueres, når vi modtager resultatet af næste modenhedsmåling ultimo 2020.

Bilag 1: Forslag til stillingsindhold for implementeringskonsulenten

Informationssikkerhedsgruppen anbefaler, at der ansættes en implementeringskonsulent til at understøtte organisationen med implementering af GDPR.

Implementeringskonsulenten skal kunne allokeres til de mest kritiske indsatsområder. Dette kan både være ud fra et strategisk perspektiv for hele organisationen eller være på center/decentralt niveau. Indsatsområderne prioriteres af KCL efter indstilling fra sikkerhedsgruppen.

Implementeringskonsulenten skal generelt understøtte de lokale sikkerhedskoordinatorer med implementering af GDPR i centrene. Implementeringskonsulenten har således en praktisk funktion i forhold til understøttelse af:

- Udarbejdelse af lokale procedurer, håndbøger, skabeloner og andet lokalt materiale
- Praktisk implementering af GDPR i centrene og understøttelse af de lokale sikkerhedskoordinatorer
- Strategisk implementeringsindsats
- Dokumentation og journalisering
- Risikovurdering
- Deltagelse i GDPR-koordinatorforum og evt. i sikkerhedsgruppen
- Sparring med de lokale sikkerhedskoordinatorer og rådgivning af centrene
- Ad hoc opgaver

Implementeringskonsulenten bør desuden have følgende personlige kvalifikationer:

- Kende den kommunale virkelighed
- Være en god kommunikator i både skrift og tale
- Være positiv, udadvendt og med gode menneskelige egenskaber
- Skal kunne finde de pragmatiske løsninger
- Være lydhøre og god til at samarbejde