INTERN REVISION

Delrapport til Databeskyttelsesrådgiverens Statusrapport for 2022

- Sundheds- og Omsorgsforvaltningen

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

1. Indledning

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance, udarbejder Databeskyttelsesrådgiveren årligt pr. 1. oktober en statusrapport.

Denne rapport er en delrapport som indeholder en vurdering af modenheden og de væsentligste risici på databeskyttelsesområdet i Sundheds- og Omsorgsforvaltningen.

2. Indsatsområder fra 2021

Vi har aftalt, en proces med forvaltningernes it-direktører omkring forvaltningernes implementering af de regler og retningslinjer som der er besluttet i forlængelse af de anbefalede indsatsområder, som fremgik af Databeskyttelsesrådgiverens statusrapport for 2021. Det blev aftalt, at medio 2023 var en rimelig frist for forvaltningerne, i forhold til at færdiggøre fortegnelse, udarbejde risikovurderingerne af behandlingsprocesserne samt udarbejde eventuelle konsekvensanalyser.

Aftalen indebærer endvidere at databeskyttelsesrådgiveren løbende giver sparring og validerer de respektive forvaltningers endelig fortegnelser, forinden processen med udarbejdelse af risikovurderinger og eventuelle konsekvensanalyser påbegyndes. Dette forventes at ske senest i december / januar 2023.

Målet er at Databeskyttelsesrådgiveren kan betrygge ledelsen i at forvaltningen har et dokumenteret og solidt overblik over de personoplysninger og behandlinger, som forvaltningen som dataansvarlig foretager og at kortlægningen i al væsentlighed er udarbejdet i overensstemmelse med kommunens regler for fortegnelsen.

Nedenfor gives en kort status på arbejdet med indsatsområderne i forvaltningen.

Fortegnelser

I Københavns Kommune er det besluttet at KLE-nummerstrukturen er udgangspunktet for forvaltningernes fortegnelser. KL Emnesystematik (KLE) er en retskildebaseret kommunal taksonomi (journaliseringsnøgle), der bruges til at registrere de kommunale opgaver.

KLE er således som udgangspunkt en bruttoliste som forvaltningerne med fordel kan tage udgangspunkt i.

Fortegnelsen skal i sin endelige form ramme enten niveau højeste niveau 1, 2 eller laveste niveau 3 i KLE-nummerstrukturen.

Forvaltningen er i proces med at udarbejde fortegnelserne. Databeskyttelsesrådgiverfunktionen har haft dialogmøder med forvaltningens eksterne konsulent omkring processen og sparring ift. opgavens omfang, anbefalinger m.v.

Vi har endnu ikke set nogle eksempler for på udarbejdede fortegnelser og har derfor ikke indblik i kvaliteten af forvaltningens fortegnelser. Vi har ligeledes ikke set et fuldstændighedsoverblik over, hvor mange fortegnelser forvaltningen påtænker at skulle udarbejde.

Vi skal gøre opmærksom på at, vi forventer at forvaltningen senest i januar 2023 har udarbejdet en fuldstændig fortegnelse for forvaltningens behandling af personoplysninger

Risikovurderinger og konsekvensanalyser

Databeskyttelsesrådgiveren tilbyder de enkelte forvaltninger individuel sparring og rådgivning i forhold til at udarbejde risikovurderinger af behandling processer samt eventuelle konsekvensanalyser.

Vi anbefaler, at forvaltningerne tager imod dette tilbud da udarbejdelse af risikovurderinger og konsekvensanalyser kan være en kompleks og ressourcekrævende opgave, hvis man ikke får den nødvendige rådgivning.

Vi forventer på nuværende tidspunkt, at forvaltningen kan påbegynde arbejdet med risikovurderinger primo februar 2023.

Tilsyn med databehandlere

Der henvises til statusrapportens afsnit 9 Indsatsområder 2021 afsnittet vedr. Tilsyn med databehandlere hvor det fremgår, at KK har tilmeldt sig som en del af Det fælleskommunale Databehandlersekretariat (DBS) som omfatter ca. 60 kommuner. Foreningen skal bistå medlemskommunerne med tilsyn og kontrol med de leverandører der anvendes at mindst 20 medlemskommuner. Det betyder at:

> *"KK og dermed forvaltningerne skal således selv udføre tilsyn med de databehandlere som ikke indgår i tilsynet hos DBS. Selv om Økonomiforvaltningen endnu ikke har udarbejdet en fællesadministrativ forretningsgang for tilsyn med databehandlere i KK, enkelte forvaltninger igangsat egne tilsyn. Vi anbefaler, at forvaltningerne afventer oplysning om hvilke databehandlere der indgår i det fælleskommunale tilsyn og derefter identificerer hvilke databehandlere der er underlagt tilsyn fra KK. Herefter bør der foretages en koordinering der sikrer mod overlap imellem forvaltningernes tilsyn og vedtages en fælles obligatorisk forretningsgang for tilsyn med databehandlere i KK, forinden tilsyn igangsættes".*

Forvaltningen har oplyst, at man har igangsat et arbejde med tilsyn med databehandlere og forventer at være færdige med opgaven, inden 2022.

Databeskyttelsesrådgiverfunktionen ikke bekendt med fremgangsmåden eller omfanget heraf, idet vi ikke har været inddraget i processen.

Oplysningspligt

Forvaltningen er i proces med at identificere de behandlingsprocesser, hvor der er krav om oplysningspligt.

Vedrørende efterlevelse af oplysningspligten vil vi i 2023 foretage et tilsyn rettet mod dette område.

Compliance i forvaltningerne

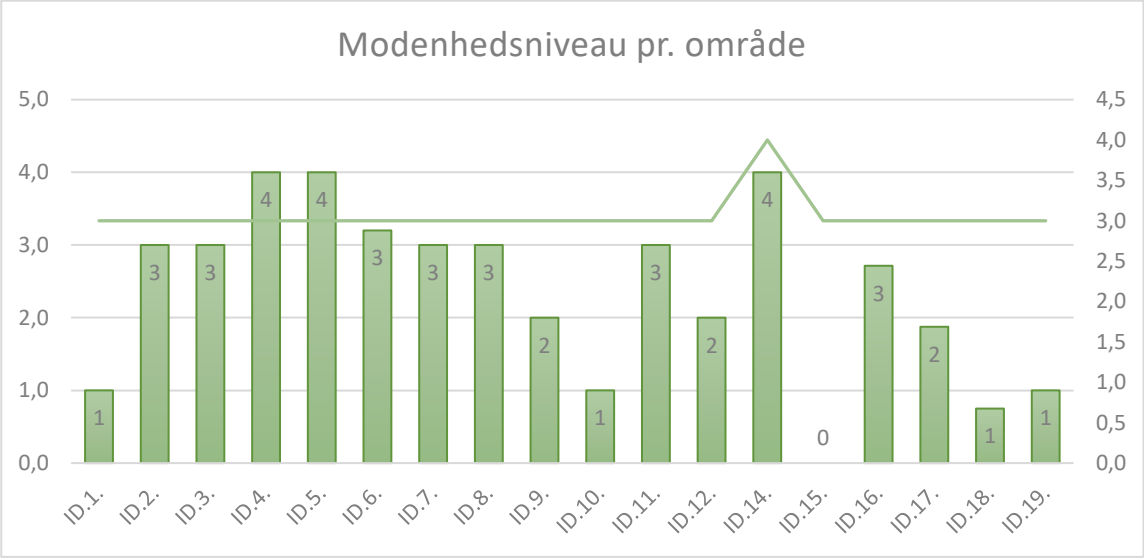
Databeskyttelsesrådgiveren etablerede i 2021 et grundlag for en modenhedsvurdering som kan anvendes til at, fastlægge en risikobaseret aktivitetsplan for både Databeskyttelsesrådgiveren og forvaltningerne fra 2022 og fremover. Formålet med modenhedsvurderingen er, at skabe transparens og prioritering i forhold til både Databeskyttelsesrådgiverens og forvaltningernes arbejde med rådgivning, undervisning og overvågning.

Hypotesen er at hvis der arbejdes bevidst med at forbedre modenheden vil man, på et oplyst grundlag, kunne reducere risikoen til et acceptabelt niveau.

Forvaltningen har i 2022 har medvirket til at justere konceptet og foretage en selvangivelse, i forhold til forvaltningens modenhed på 46 complianceområder. Resultatet fremgår af næste afsnit.

Modenhed i forvaltningen

Forvaltningen har en række kritiske områder, hvor det kræves, at forvaltningen styrker modenheden. Derudover er der flere indsatsområder, som forvaltningen kan inddrage i det kommende års aktivitetsplan.



Graften illustrer at forvaltningen i de fleste tilfælde har udarbejdet retningslinjer, der dækker de overordnede hovedområder.

Complianceområder henhører alle under hver deres hovedområde. Et hovedområde er således en henvisning til, hvad de underliggende complianceområder vedrører.

Et hovedområde kan f.eks. være "Medarbejdersikkerhed før, under og efter ansættelsen", " Mobilt udstyr og fjernarbejdspladser" m.v. Alle hovedområder har et ID.nr. som overskueliggøre rapporteringen, men som ligeledes sikrer fortrolighed omkring tekniske indretninger samt drift eller forretningsforhold – eller mangler deraf – som muligvis vil kunne udnyttes, med væsentlig økonomisk betydning for kommunen.

Forvaltningernes selvangivelser vil over tid derfor blive efterprøvet i takt med, at Databeskyttelsesrådgiveren afslutter et tilsyn på et givent complianceområde. Dette kan eventuelt medføre justeringer i op eller nedadgående retning, på modenhedsskalaen, alt efter tilsynets udfald sammenlignet med forvaltningens egen selvangivelse.

På områder, hvor forvaltningerne er umodne, og altså ikke klar til egentlige tilsyn, vil der være en periode, hvor forvaltningerne kan bringe området op til et forventet "modenhedsminimum". Dette vil efterfølgende skulle afspejles i forvaltningernes aktivitetsplaner, der ud fra en risikobaseret tilgang, arbejder med de enkelte udeståender.

Konceptet vil derfor kunne understøtte forvaltningernes fremadrettede arbejde, ud fra en mere compliance-og risikobaseret tilgang ift. databeskyttelse.

Konceptet vil ligeledes kunne understøtte forvaltningernes ledelsesrapportering, da det vil give et grundigt overblik over databeskyttelsesmodenheden år for år.

Brug af konceptet er et tilbud og ikke et krav. Konceptet vil løbende blive justeret, hvis der opdages uhensigtsmæssigheder eller andre forbedringspotentialer.

Det er vigtigt at være opmærksom på, at man ikke nødvendigvis skal have en score på 4 eller 5, før et modenhedsniveau er tilfredsstillende. I langt de fleste tilfælde vil et modenhedsniveau på 3 være tilstrækkeligt. Dette afhænger meget af complianceområdet og fastsættes til dels af Databeskyttelsesrådgiveren ud fra en objektiv vurdering – med afsæt i konceptets vurderingsprincipper.

At løfte niveauet på de kritiske og umodne compliance områder kan som udgangspunkt håndteres ved at udarbejde regler og retningslinjer, og det er vores vurdering, at kommunen med en begrænset central indsats kan løfte de anførte kritiske og umodne complianceområder.

Grundet offentliggørelsen af Databeskyttelsesrådgiverens Statusrapport, herunder også den konkrete delrapport, vil der ikke blive foretaget en yderligere uddybning af de enkelte områder, idet dette kan udgøre en sikkerhedsrisiko for kommunen.

Forvaltningen er gjort bekendt med de specifikke indsatsområder.