INTERN REVISION

STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

For perioden 1.oktober 2019 til 1.oktober 2020

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Indledning

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance, udarbejder Databeskyttelsesrådgiveren årligt pr. 1. oktober en statusrapport. Rapporten indeholder en vurdering af databeskyttelsen samt øvrige forhold i relation til databeskyttelse i Københavns Kommune.

Rapporten fremsendes til forvaltningernes direktioner, til Revisionsudvalget og til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

I § 12-erklæringen vedr. statusrapporten 2019 angav ØKF bl.a.:

"Økonomiudvalget bemærker, at der alene foreligger en statusrapport, som omfatter kommunen som helhed. Økonomiudvalget har noteret sig, at Databeskyttelsesrådgiveren i indledningen, side 2, har beskrevet, at baggrunden herfor er, at risikovurderingerne stort set er identiske for de enkelte forvaltninger i 2019. Økonomiudvalget forventer, at der i takt med opbygning af erfaringer på området fremadrettet vil foreligge risikovurderinger pr. forvaltning og for kommunen som helhed, som det fremgår af funktionsbeskrivelsen."

Der foreligger på nuværende tidspunkt ikke en risikovurdering for de enkelte forvaltninger. Derfor er der i lighed med 2019 kun udarbejdet en rapport for kommunen som helhed, der omhandler arbejdet med databeskyttelse i perioden 1.oktober 2019 til 1. oktober 2020. Der henvises til rapportens pkt. 2.2. Risikovurderingskoncept, for yderligere oplysninger om arbejdet med risikovurderinger.

2. Status

2.1. Den overordnede status for databeskyttelse i Københavns Kommune

Samlet set er det Databeskyttelsesrådgiverens vurdering:

- at Københavns Kommune på nuværende tidspunkt har en klar og tydelig rolle- og ansvarsfordeling samt passende regler og retningslinjer, der medvirker til at sikre en betryggende databeskyttelse i Københavns Kommune.

- at de databeskyttelsesretlige regler administreres på et fornuftigt grundlag i Københavns Kommune. Databeskyttelsesrådgiveren er ikke bekendt med områder, hvor der ikke er fokus på databeskyttelse.

- at alle ledelseslag i Københavns Kommune arbejder bevidst med og respekterer de databeskyttelsesretlige regler.

- at der er den nødvendige opbakning og forståelse for Databeskyttelsesrådgiver-funktionens rolle og ansvar.

I statusrapporten for 2019 pegede Databeskyttelsesrådgiveren på nogle konkrete forhold, der burde forbedres for at sikre den nødvendige fremdrift i databeskyttelsen i Københavns Kommune.

De konkrete forhold der blev peget på, var:

- koordinering af den samlede indsats på databeskyttelsesområdet
- overblik over udmøntningen/operationalisering af ansvarsområder
- overblik over de ressourcer, der anvendes samlet i Kommunen på databeskyttelse

Efter drøftelse og godkendelse i IT-kredsen tog Databeskyttelsesrådgiveren i januar 2020 initiativ til at opstarte en række arbejdsgrupper, som skulle håndtere Databeskyttelsesrådgiverens observationer og anbefalinger. Forvaltningerne var repræsenteret i arbejdsgrupperne via DPO Business partnerne og Vejledende Sikkerhed i Koncern IT.

Følgende værktøjer/materialer skulle udarbejdes:

- Uddybende funktionsbeskrivelser for DPO Business Partner, Vejledende Sikkerhed og Databeskyttelsesrådgiveren (Værktøj 1), som består af:
    - Bilag 1 – Uddybende funktionsbeskrivelse Databeskyttelsesrådgiver
    - Bilag 2 – Uddybende funktionsbeskrivelse – Vejledende Sikkerhed
    - Bilag 3 – Uddybende funktionsbeskrivelse DPO Business Partner
    - Bilag 4 - Snitflade-og opgavebeskrivelsesoverblik

- Værktøj 2 – Årshjul og aktivitetsplaner, som består af:
    - Bilag 5 - Skabelon for Aktivitetsplan
    - Bilag 6 - Procesbeskrivelse Årshjul og aktivitetsplaner

- Værktøj 3 – Tilsyn, som består af:
    - Bilag 8 - Procesbeskrivelse for tilsyn
    - Bilag 9 – Tilsynsorienteringsskabelon
    - Bilag 10 – Skabelon for tilsynsrapport

- Værktøj 4 – Journalisering og dokumentation, som består af:
    - Bilag 7 – Procesbeskrivelse for journalisering og dokumentation (DPO BP)

Arbejdet for fire af arbejdsgrupperne blev afsluttet maj måned 2020. Grundet Covid-19 blev arbejdet afsluttet senere end forventet.

Den 23. oktober 2020 godkendte IT-kredsen:

- Uddybende funktionsbeskrivelse for forvaltningens DPO Business Partner (værktøj 1)
- Fællesadministrativ forretningsgang for årshjul og aktivitetsplan på databeskyttelsesområdet (værktøj 2). Forud for dette forslag blev graden af fælles aktivitet- og tidsstyring drøftet mellem Databeskyttelsesrådgiveren og forvaltningernes DPO Business Partnere. Der var tilslutning til tæt koordination på aktivitetsområdet med et fælles årshjul og dertilhørende aktivitetsplaner.

Arbejdet med værktøj 3 om tilsyn viste, at snitfladen mellem DPO'en og forvaltningerne på enkelte områder kunne tolkes forskelligt, herunder særligt på it-tilsynsområdet. På den baggrund aftaltes det den 11. september 2020 mellem IT-kredsen og Databeskyttelsesrådgiveren, at der sker en præcisering således, at det formaliserede tilsyn med overholdelsen af de databeskyttelsesretlige regler på tværs af alle forvaltninger, foretages af Databeskyttelsesrådgiveren. Forvaltningerne foretager almindeligt ledelsestilsyn som led i forvaltningens arbejde med databeskyttelse. IT-kredsen godkender samtidig, at der i forbindelse med opgaveflyttet permanent tilføres to årsværk til Databeskyttelsesrådgiveren.

- Under drøftelserne vedrørende værktøj 4 – Journalisering og dokumentation (DPO BP) var det forvaltningernes vurdering, at de eksisterende vejledninger og retningslinjer for journalisering i Københavns Kommune dækker databeskyttelsesområdet, og at værktøj 4 derfor ikke vurderes relevant at implementere.

Databeskyttelsesrådgiveren tager til efterretning at der ikke kunne opnås tilslutning til forslaget om at skabe et overblik over de samlede ressourcer, der er til rådighed og anvendes til databeskyttelse ligesom der ikke var opbakning til en særlig journalisering og dokumentation af DPO Business Partnernes arbejde.

Herudover er der taget initiativ til, at Økonomiforvaltningen i samarbejde med DPO Business Partner Forum og digitaliseringscheferne udarbejder et kommissorium for DPO Business Partner Forum, der fremover i tæt samarbejde med Databeskyttelsesrådgiveren får til opgave at varetage koordineringen af databeskyttelsesindsatser i kommunen, herunder koordinering af forvaltningernes aktivitetsplaner og årshjul og prioritering, tilrettelæggelse og udførelse af tværgående complianceindsatser.

Endelig er det besluttet at DPO Business Partnere fremover betegnes med en mere sigende titel. Databeskyttelsesrådgiveren og forvaltningerne har oplevet forveksling mellem Databeskyttelsesrådgiveren og forvaltningernes DPO Business Partnere. Dette sammenholdt med de ændringer om roller og ansvar, der seneste er aftalt, gør, at det er besluttet at titlen fremover er GDPR Business Partner.

Databeskyttelsesrådgiverens ser frem til at der for 2021 foretages en koordinering af den samlede operationelle indsats i Københavns Kommune på databeskyttelsesområdet.

2.2. Risikovurderingskoncept

Af Databeskyttelseslovgivningen fremgår det, at den dataansvarlige (Københavns Kommune) skal udvise ansvarlighed i enhver henseende i forhold til de registreredes (borgere, medarbejder mv.) personoplysninger. Det er desuden et krav, at de foranstaltninger, der skal sikre denne ansvarlighed er baseret på en risikovurdering. En risikovurdering skal identificere risikoen for de registreredes rettigheder og frihedsrettigheder ved enhver behandling af personoplysninger.

Databeskyttelsesrådgiveren vurderede i 2019, at kommunens største risiko er, at der ikke i tilstrækkelig grad arbejdes risikobaseret. I samarbejde med Koncern IT har Databeskyttelsesrådgiveren igangsat et projekt der skal medvirke til at skabe overblik, forståelse og effektivitet i kommunens risikovurderingsproces:

1. OVERBLIK

En fælles tilgang til risikostyring på tværs af enheder i kommunen.

2. FORSTÅELSE

Indsigt i samspillet mellem risici for forretning, it og privatlivet.

3. EFFEKTIVITET

En nemmere proces til identificering og kvalificering af risici.

Projektet gennemføres med ekstern bistand og de relevante enheder i kommunen som arbejder med risikovurderinger, inddrages i arbejdet med optimering og samordning af de nuværende modeller. Risikovurderingskonceptet udarbejdes i overensstemmelse med ISO-standarderne.

Grundet Covid-19 forventes arbejdet at blive afsluttet i slutningen af Q1 2021 og implementeret i løbet af 2021.

Databeskyttelsesrådgiveren ser frem til at der fremadrettet implementeres en ensartet og standardiseret risikovurdering på hele informationssikkerhedsområdet på tværs af alle enheder således at indsatsen (foranstaltningerne) bliver mere effektive i forhold til at reducere de identificerede risici.

2.3. Henvendelser til Databeskyttelsesrådgiveren

Databeskyttelsesrådgiveren ønsker at blive opfattet som en ressource frem for en autoritet, selv om opgaverne også omfatter overvågning og tilsyn samt rapportering heraf til BR, ØU og forvaltningernes ledelse. Det er den umiddelbare vurdering, at forvaltningerne er gode til at kontakte Databeskyttelsesrådgiveren, når der er behov for det.

Siden 1. oktober 2019 har Databeskyttelsesrådgiveren ført statistik med, hvor mange henvendelser der har været fra de enkelte forvaltninger. Henvendelserne giver Databeskyttelsesrådgiveren et indblik i, hvordan de databeskyttelsesretlige regler forvaltes. En henvendelse bliver registreret, når Databeskyttelsesrådgiveren kontaktes for rådgivning og vejledning.

Nedenstående tabel viser henvendelser fra den 1.oktober 2019 til 1.oktober 2020.

Forvaltning	**Antal henvendelser**
Beskæftigelses-og Integrationsforvaltningen	16
Børne-og Ungdomsforvaltningen	28
Kultur-og Fritidsforvaltningen	25
Socialforvaltningen	39
Sundheds-og Omsorgsforvaltningen	19
Teknik-og Miljøforvaltningen	19
Økonomiforvaltningen	32

Databeskyttelsesrådgiveren opfordrer til at forvaltningerne ikke er tilbageholdende med at kontakte Databeskyttelsesrådgiver-funktionen, da det er med til at skabe opmærksomhed på tværgående problemstillinger og indblik i forvaltningsspecifikke udfordringer m.v.

3. Afgørelser fra Datatilsynet

Fremadrettet vil Databeskyttelsesrådgiveren i statusrapporterne orientere om væsentlige afgørelser og henvendelser fra Datatilsynet. Der henvises endvidere til afsnit 4.2 vedrørende sager om persondatabrud.

3.1. Anvendelse af SharePoint

Den 15. oktober 2019 udtalte Datatilsynet **alvorlig kritik** af Københavns Kommune for den behandling, som havde fundet sted i SharePoint. Datatilsynet undersøgte en specifik behandling og der var derfor ikke udtryk for en generel undersøgelse af al behandling i SharePoint.

I den specifikke sag var behandlingen ikke sket i overensstemmelse med databeskyttelsesforordningens artikel 32. Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de identificerede risici. Til dette udtalte Datatilsynet, at Københavns Kommune ikke i tilstrækkeligt omfang havde iagttaget denne bestemmelse.

Datatilsynet lagde bl.a. vægt på, at flere medarbejdere, end hvad der måtte anses for værende nødvendigt, havde haft adgang til de filer sagen vedrørte, samt at Københavns Kommune havde en omfattende mængde filer i SharePoint, herunder filer med oplysninger af fortrolig og følsom karakter. Datatilsynet lagde desuden vægt på at den etablerede logning og de oplyste interne retningslinjer om, at følsomme og fortrolige oplysninger ikke må opbevares i endelig dokumentform på fælles drev i mere end 30 dage, ikke i sig selv udgør tilstrækkelig grad af sikkerhed, og derfor ikke kunne anses for at udgøre en passende sikkerhedsforanstaltning.

Det var derfor Datatilsynets opfattelse at personoplysninger, der behandles i SharePoint, hurtigst muligt – efter en risikovurdering – skulle overføres til København Kommunes sagsbehandlingssystem.

Københavns Kommune har efterfølgende igangsat et omfattende oprydningsarbejde i SharePoint og etableret en governance struktur, der skal skabe grundlag for den løbende vedligeholdelse af SharePoint.

3.2. CPR-abonnementer

Datatilsynet har den 25. oktober 2019 udtalt **kritik** af Københavns Kommune i forbindelse med at kommunen har abonneret på CPR-oplysninger om en borger, som ikke har haft bopæl i Københavns Kommune siden 1999.
På baggrund af borgerens første henvendelse konkluderede Københavns Kommune, at man ikke havde behov for at behandle borgerens CPR-nummer og abonnementet hos Det Central Personregister blev derfor opsagt.

Efterfølgende viste det sig, at abonnementet på oplysninger om klager i CPR automatisk var blevet gentegnet, fordi der i kommunens journaliseringssystemet var registreret en aktuel sag vedrørende klager, som var blevet oprettet på baggrund af klagers henvendelse af 17. januar 2018 om kommunens abonnering af oplysninger om ham.

Københavns Kommune angav som begrundelse for at genoptage CPR-abonnementet, at det var nødvendigt at oprette et CPR-abonnement med henblik på entydig identifikation og som journalnummer så kommunen havde retvisende og aktuelle identifikationsoplysninger om borgeren for bl.a. at kunne håndtere eventuelle aktindsigts- eller rettighedsanmodninger, eller andre retskrav, efter bl.a. offentlighedsloven, forvaltningsloven og databeskyttelsesreglerne.

Datatilsynet udtalte på den baggrund, at behandling af oplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, skal være *nødvendig*. Efter Datatilsynets opfattelse anses det ikke for nødvendigt, at oprette automatiske personabonnementer i CPR med det formål at kunne håndtere eventuelle aktindsigts- eller rettighedsanmodninger, idet man i kommunen har mulighed for at lave enkeltopslag i CPR, når der viser sig et aktuelt behov for at ajourfører personoplysninger.

Udtalelsen konkluderer, at CPR-abonnementer kun må oprettes, hvis der er et sagligt behov herfor. Ligesom aktive abonnementer løbende skal slettes, når der ikke længere er et sagligt behov for at modtage oplysninger fra Det Central Personregister.

På baggrund af udtalelsen blev det besluttet, at

- CPR-abonnementer på borgere i KK slettes snarest (17.099 abonnementer)
- CPR-abonnementer på udenbys borgere slettes ultimo januar 2020, efter opgraderingen af kommunens ESDH-system (230.730 abonnementer)

3.3. Mangel på oplysningspligt

Datatilsynet har den 4.september 2020 udtalt **kritik** af Københavns Kommunes Børne-og Ungdomsforvaltning fordi oplysningspligten, ikke var iagttaget i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 13, jf. artikel 12, stk. 1.

Opfyldelse af oplysningspligten er en vigtig grundrettighedsbeskyttelse i databeskyttelsesforordningen, da den sikrer gennemsigtighed overfor borgerne.

Datatilsynet udtaler:

"Efter databeskyttelsesforordningens artikel 13, stk. 1, skal den dataansvarlige, på det tidspunkt hvor oplysningerne indsamles, give den registrerede alle de oplysninger der fremgår af artikel 13, stk. 1 og 2. Oplysningerne skal gives i den form og på den måde der fremgår i artikel 12, stk. 1.

I overensstemmelse med det af Københavns Kommune Børne- og Ungeforvaltningen erkendte, lægges det til grund, at de påkrævede oplysninger, ikke er givet til klager på tidspunktet hvor oplysningerne blev indhentet."

Det er ikke Databeskyttelsesrådgiverens umiddelbare oplevelse, at forvaltningerne ikke generelt efterlever oplysningspligten overfor borgerne. Databeskyttelsesrådgiveren vil på baggrund af udtalelsen og et observeret eksempel foretage tilsyn med forvaltningernes efterlevelse af oplysningspligten i 2021.

3.4. Tilsyn med Robotic Proces Automation (RPA) og Kunstig Intelligens (AI)

Datatilsynet varslede den 17. januar 2020 Københavns Kommune et tilsynsbesøg. Emnet var Robotic Proces Automation (RPA) og Kunstig Intelligens (AI). Forud for mødet skulle kommunen udarbejde en liste med:

- Alle systemer der benytter RPA teknologi, fordelt på forvaltningsområder
- På de identificerede systemer, skal der i punktform, fremgå en beskrivelse af hvilke oplysninger der behandles, behandlingshjemmel samt i hvilket omfang den brugte automatisering danner grundlag for nye registreringer i sagsbehandlings- eller andre fagsystemer

- Alle systemer der – i ordets bredeste forstand – benytter AI. Dette omfatter også systemer der måtte benyttes til ledelsesinformation og systemer der benytter data på aggregeret niveau, uanset om data af kommunen selv anses for anonymiseret.
- På de identificerede systemer, skal der i punktform, fremgå en beskrivelse af hvilke oplysninger der behandles, behandlingshjemmel samt i hvilket omfang den brugte logik og resultaterne heraf, danner grundlag for nye afgørelser og/eller registreringer i sagsbehandlings- eller andre fagsystemer

Koordineringen i forbindelse med tilsynet blev varetaget af ØKF/KIT og Databeskyttelsesrådgiveren.

Tilsynsbesøget blev afholdt den 24. februar 2020.
Under mødet var repræsentanter fra de forvaltninger, som ejede systemerne BUF, BIF og SOF, og KIT.

Københavns Kommune er forsat i proces med Datatilsynet. Det forventes, at der kan gå op til et år, før tilsynet er afsluttet. Det er på nuværende tidspunkt ikke muligt at vurdere, hvilket udfald tilsynet vil få for Københavns Kommune.

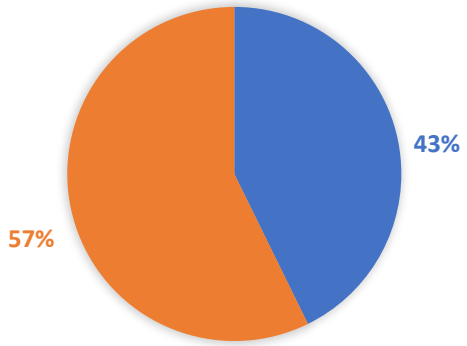
4. Persondatabrud

Det er Databeskyttelsesrådgiverens opfattelse, at forvaltningerne har en god proces for håndteringen og koordineringen af persondatabrud, samt at medarbejderne har en god forståelse af, hvad et persondatabrud er samt evnen til at identificere hændelser. Databeskyttelsesrådgiveren vil foretage tilsyn på området i 2021.

Databeskyttelsesrådgiveren oplever forsat, at antallet af brud på tværs af kommunens forvaltninger varierer en del.

I perioden 1. juli 2019 til den 1. oktober 2020 er der blevet registeret 593 persondatabrud i Københavns Kommune.

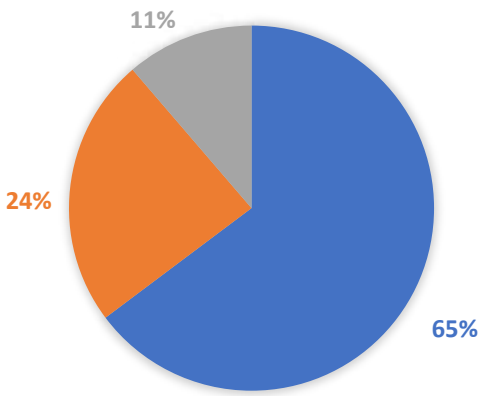
Figur 1. Sager der har været anmeldt til Datatilsynet i det tilfælde sagen har haft karakter af et persondatabrud:



Viser antal sager (272), hvor forvaltningen har vurderet, at der ikke har været behov for at anmelde sagen til Datatilsynet.

Viser antal sager (203), hvor forvaltningen har vurderet, at sagen skal anmeldes til Datatilsynet.

Figur 2. Fordeling af, hvorvidt sagerne har haft karakter af persondatabrud eller ej, samt ikke afsluttede sager:



Viser antal sager (67), som endnu ikke er afsluttet.

Viser antal sager (384), hvor forvaltningerne har vurderet, at der var tale om et persondatabrud.

Viser antal sager (142), hvor forvaltningerne har lukket sagen, fordi det er blevet vurderet, at der ikke var tale om et persondatabrud.

De hyppigste årsager til persondatabrudende er forsat hændelser, som resulterer i utilsigtet videregivelse på grund af menneskelige fejl.

Databeskyttelsesrådgiveren foretager tilsyn med forvaltningernes indsats rettet mod at undgå gentagelse af persondatabrud i 2021, samt den konkrete håndtering.

4.1. Alvorlig kritik - Sagerne gengivet i kort resumé

Hvad Databeskyttelsesrådgiveren har kendskab til, har Københavns Kommune i alt modtaget 97 afsluttende breve fra Datatilsynet for indberettede persondatabrud siden 1. juli 2019 til 1. oktober 2020.

I 94 af sagerne har der ikke været anledning til udtalelse fra Datatilsynet. I 2 sager har Københavns Kommune modtaget alvorlig kritik, samt 1 udtalelse med kritik.

Den første sag vedrører implementeringen af et system i Københavns Kommune. I den forbindelse foretog man nogle test af produktionsmiljøet, hvor man benyttede oplysninger fra en række testpersoner, som havde underskrevet en samtykkeerklæring på, at deres personoplysninger måtte bruges til test. Alle var ansatte i Københavns Kommune og der var tale om ca. 14 medarbejdere. Da man overgik til drift, havde man ikke fået slettet alle testoplysningerne, hvilket fik retsvirkende konsekvenser for medarbejderen, som i øvrigt ikke havde givet samtykke til at vedkommendes oplysninger blev brugt til test.

Den anden sag vedrørte manglende kontrol med brugerautorisationer i forbindelse med skiftende opgavevaretagelse og stillingsbetegnelse. Dette bevirkede, at medarbejderen havde autorisationer til at foretage ændringer i systemet, som denne ikke burde have været tillagt. Der var tale om medicinsk behandling, hvilket kræver særlig opmærksomhed ift. håndteringen og kommunens kontrolforanstaltninger.

I begge henseender lagde Datatilsynet vægt på, at Københavns Kommune ikke havde truffet de nødvendige tekniske og organisatoriske foranstaltninger, hvilket understreger behovet for brugen af risikovurderinger fremadrettet til at kunne dokumentere tiltag m.v.

Forvaltningerne har udarbejdet handleplaner for at sikre, at lignende tilfælde ikke gentages. Databeskyttelsesrådgiveren foretager en opfølgning på forvaltningens handleplaner i 2021.

5. Databeskyttelsesrådgiverens afsluttede opgaver

5.1. KK "Benspændskatalog"

I januar 2020 meldte Kommunernes Landsforening (KL) ud at: "GDPR spænder ben for velfærden. Hver eneste dag slås landets kommuner nærmest helt bogstaveligt med implementeringen af den nye databeskyttelsesforordning, i daglig tale blot kaldet GDPR".

KL havde i den forbindelse samlet et udsnit af eksempler på, hvordan GDPR efter kommunernes opfattelse spænder ben for kommunernes arbejde. Med det nye benspændskatalog i hånden ville KL tage sagen op med regeringen og EU.

Datatilsynet offentliggjorde kort efter en publikation, hvor Datatilsynet gennemgik og besvarede KL's eksempler. En stor del af de eksempler, som KL havde anført i "benspændskataloget", er ikke benspænd, men mere basale borgerrettigheder, ifølge Datatilsynet.

Datatilsynet anførte i den forbindelse, at det gælder generelt for reglerne i GDPR, at de er fleksible og kan tilpasses de mange forskellige situationer, hvor man behandler personoplysninger. Datatilsynet tilføjede, at det til gengæld også betyder, at reglerne ikke tager stilling til konkrete scenarier og teknologier, og at man som dataansvarlig selv skal foretage en vurdering af, hvad der er nødvendigt og rimeligt over for borgerne. Datatilsynet anerkendte i den forbindelse at det kan være svært for den enkelte medarbejder på et plejehjem, i en børnehave e.l. at skulle forholde sig til juraen. Datatilsynet foreslog derfor, at man lader kommunens jurister sætte rammerne for arbejdet.
I kølvandet på KL's "benspændskatalog" og de eksempler vi har set i forbindelse med KL's erfaringsindsamling, har Databeskyttelsesrådgiveren igangsat et arbejde med at opspore eventuelle "benspænd" fra databeskyttelseslovgivningen i Københavns Kommune, ved at opfordre alle kommunens ansatte til at fremsende de udfordringer i forhold til databeskyttelse, de oplever i hverdagen.

Dette vil der blive arbejdet på i Q4 2020. Resultatet bliver et katalog, der håndterer hverdagsproblemstillinger, som f.eks. kan være, om der må hænge billeder af børn i en institution og lignende.

5.2. Tilsyn med Uddannelsesplaner

Databeskyttelsesrådgiveren afsluttede i september måned 2019 sit tilsyn med forvaltningernes uddannelsesplaner. Tilsynet omfattede en gennemgang af, hvorvidt forvaltningerne havde lavet et design der sikrer, at de ansatte modtager en relevant uddannelse i håndteringen af personoplysninger, hvorvidt dette design har været implementeret tilstrækkeligt (kendt af de ansatte og ledelserne), samt hvorvidt design og proces fungerer effektivt, altså om det tilsigtede resultat opnås.

Tilsynet blev gennemført for alle syv forvaltninger.

De vigtigste observationer viste bl.a., at:

- retningslinjerne var designet i tilstrækkelig grad i flere af forvaltningerne, dog måtte enkelte forvaltninger genbesøge uddannelsesplanen
- implementeringen af retningslinjerne var mangelfuld i flere forvaltninger

- I flere forvaltninger modtog et større antal ansatte ikke undervisning i håndtering af persondatabrud
- Generelt set var der var manglende ledelsesmæssig opfølgning på om de ansatte havde gennemført uddannelsen eller ej
- data i uddannelsessystemet ikke blev holdt tilstrækkeligt vedlige ift. hvorvidt medarbejderne var ansat i forvaltningerne

Databeskyttelsesrådgiveren igangsætter en opfølgning for sidste års tilsynsrapport Q4 2020. Dette sker i forbindelse med, at det er 2 år siden størstedelen af Københavns Kommune sidst modtog undervisning, og at frekvensen for uddannelse netop er fastsat til 2 år.

6. National evaluering af databeskyttelsesreglerne

Databeskyttelsesforordningen og den supplerende databeskyttelseslov har været gældende siden den 25. maj 2018. Som led i en national evaluering af databeskyttelsesreglerne vil Justitsministeriet undersøge mulighederne for at begrænse anvendelsen af databeskyttelsesforordningen og forenkle reglerne i databeskyttelsesloven på særligt udvalgte områder.

Ifølge Justitsministeriets udkast til en procesplan for en national evaluering af databeskyttelsesreglerne vil ministeriet afdække mulighederne for at lempe disse. Den nationale evaluering skal udarbejdes med afsæt i dels en erfaringsindsamling fra relevante interessenter, dels en række juridiske undersøgelser, som foretages af Justitsministeriet selv.

Erfaringsindsamlingen vil ske ved en bred høring af relevante interessenter herunder kommuner. Formålet med høringen er blandt andet at få belyst de konkrete situationer, der er uklare og giver anledning til tvivl, når databeskyttelsesreglerne skal efterleves i praksis.

Formålet med de juridiske undersøgelser, der skal foretages af Justitsministeriet selv, er blandt andet at belyse mulighederne for henholdsvis:

- at begrænse databeskyttelsesforordningens anvendelse på "mindre aktører, herunder frivillige foreninger"
- at indføre en påbudsordning, hvorefter Datatilsynet i videre omfang skal meddele påbud, før Datatilsynet anmelder den dataansvarlige virksomhed, forening, myndighed mv. til politiet med indstilling om bøde, eller før der udstedes et administrativt bødeforelæg
- at indføre en ordning, hvorefter tilsynsmyndigheden på anmodning kan afgive udtalelse om sin vurdering af lovligheden af en påtænkt aktivitet, der indebærer en behandling af personoplysninger
- at forenkle reglerne i databeskyttelsesloven.

Evalueringen forventes færdiggjort primo 2021.

Databeskyttelsesrådgiveren vil i 2021 have fokus på eventuelle ændringer som påvirker Københavns Kommunes indsats på databeskyttelsesområdet.

7. Selvejende institutioner med driftsoverenskomst

I Københavns Kommune er det besluttet at kommunens Databeskyttelsesrådgiver også kan fungere som Databeskyttelsesrådgiver for de selvejende institutioner med driftsoverenskomst. Denne funktion DPOSI fungerer p.t. som databeskyttelsesrådgiver for 153 selvejende institutioner fordelt på 220 lokationer.

I første kvartal af 2020 er Legal Complianceprojektet for de selvejende institutioner afsluttet. Projektet er gennemført på 12 måneder, der er anvendt 9.714 timer. Både timer og varighed er under budget. I projektet er der afholdt 418 møder med institutionerne og gennemgået mere end 300 dokumenter i form af databehandleraftaler, samtykker mv. Hver af de 160 institutioner har modtaget en afsluttende compliancerapport, som har givet institutionen indsigt i deres complianceniveau og et springbræt til forbedringer.

DPOSI har gennem året fokuseret på at understøtte institutionerne i den reelle implementering af GDPR. Dette er sket gennem en "en-til-en" rådgivning på væsentlige områder og en gennemgang af dokumenter, der er et krav for institutionerne anvende, samt en uddannelsesdag for 100 institutioner. Målet har været at gøre institutionerne klar til at overgå til drift og at etablere en solid governance med afsæt i DPOSI's anbefalinger og værktøjer. DPOSI har modtaget 1-2 henvendelser om dagen med spørgsmål, hvoraf der har været 46 større rådgivningssager.

Det har været væsentligt for DPOSI at skabe et omdømme som tilgængelig og effektiv rådgiver. Derfor har DPOSI lagt vægt på at besvare alle henvendelser hurtig, og at sikre praktiske og forståelige anbefalinger. Det har desuden været væsentligt at få opbygget et tillidsfuldt samarbejde, hvor institutionerne er komfortable med at søge hjælp og har en positiv indstilling til tilsynsaktiviteter i det kommende år.

Sideløbende med de kunderettede aktiviteter har DPO brugt året til at færdigudvikle en samlet proces, et framework og værktøjer for DPO-funktionens arbejde. Dette er baseret på de erfaringer, der er indsamlet i Legal Complianceprojektet og med ISO-standarder som grundlag.

København, den 30. november 2020

Københavns Kommune Databeskyttelsesrådgiverfunktion

Jesper Gjøtterup Andersen

Databeskyttelsesrådgiver for Københavns Kommune

Nicholai Mandrup	Line Nymann Schoop	Christian Sonn Kjelmann
Lone Forsberg	Jonathan Brix	Io Alexandra Sarroe-Brinkløv