STATUSRAPPORT

Databeskyttelsesrådgiveren

November 2019

Statusrapport om Københavns Kommunes arbejde med databeskyttelse

25. maj 2018 til 1. oktober 2019

MODTAGER

Revisionsudvalget
Borgerrepræsentationen

Indholdsfortegnelse

1. INDLEDNING

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance udarbejder Databeskyttelsesrådgiveren årligt pr. 1. oktober en statusrapport som indeholder en risikovurdering suppleret med en kort vurdering af complianceniveauet, omfanget af sikkerhedsbrud 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.

Denne rapport er den første, der er udarbejdet. Idet risikovurderingerne stort set er identiske for de enkelte forvaltninger, er der i 2019 kun udarbejdet en rapport for kommunen som helhed, der omhandler arbejdet med databeskyttelse i perioden 25. maj 2018 til 1. oktober 2019.

Endvidere giver Databeskyttelsesrådgiveren sine anbefalinger til, hvordan efterlevelsen af databeskyttelseskrav forbedres i den kommende periode.

Rapportens datagrundlag er indhentet fra bl.a. Datatilsynet og Københavns Kommunes It (KIT). Rapportens konklusioner og anbefalinger er drøftet med forvaltningerne.

2. STATUS

2.1 Den overordnet status på efterlevelse af Københavns Kommunes databeskyttelseskrav

Økonomiudvalget varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it- og informationssikkerhedsforhold. Udvalget har besluttet at enhver håndtering af personoplysninger og værdioplysninger i Københavns Kommune skal ske på en betryggende og tillidsvækkende måde i forhold til kommunens borgere og virksomheder, og at kommunen følger de regler for behandling af personoplysninger, der er fastsat i Databeskyttelsesforordningen og Databeskyttelsesloven.

I overensstemmelse med databeskyttelseslovgivningen skal kommunen udpege en Databeskyttelsesrådgiver. I København er databeskyttelsesrådgiverfunktionen forankret i Intern Revision som en uafhængig enhed med direkte reference til Borgerrepræsentationen. Dette skete i umiddelbar forlængelse af Borgerrepræsentationens beslutning i april 2016 om iværksættelse af en handlingsplan for styrkelse af it- sikkerheden.

I samme forbindelse blev der truffet beslutning om et kommissorium for gennemførelse og implementering af et legal complianceeftersyn i 2016 – 2018 af kommunens it-sikkerhed og behandling af personoplysninger på tværs af kommunens forvaltninger. Dette med henblik på implementering og opfyldelse af databeskyttelseslovgivningen frem mod forordningens ikrafttrædelse den 25. maj 2018.

I forlængelse heraf organiserede kommunen sig med en DPO Business Partner i hver forvaltning. Business Partneren er kontaktpunkt til Databeskyttelsesrådgiveren og er forvaltningernes (dataansvarlig) vidensperson indenfor databeskyttelsesområdet. Rollen og ansvaret er sammen med KIT's rolle formaliseret og uddybet i cirkulærer og fællesadministrative forretningsgange. Business Partneren skal til stadighed vurdere complianceniveauet i forvaltningen og skal gennem en direkte adgang til forvaltningens ledelse underrette om dette. Endvidere skal Business Partneren proaktivt arbejde for, at forvaltningens complianceniveau lever op til lovgivning og regler gennem rådgivning af og samarbejde med forvaltningens medarbejdere.

Ovenstående har været stærkt medvirkende til at Københavns Kommune fik et godt udgangspunkt i forhold til at efterleve de regler for behandling af personoplysninger, der er fastsat i Databeskyttelsesforordningen og Databeskyttelsesloven.

Legal Compliance Projektet, som var et implementeringsprojekt, er nu afsluttet og forvaltningernes Business Partner og Databeskyttelsesrådgiveren er nu almindelige driftsfunktioner.

De første 1,5 år er primært gået med at få styr på reglerne, udarbejde retningslinjer, designe og implementere regler, retningslinjer og forretningsgange og uddanne medarbejdere.

Flere væsentlige forretningsgange vurderes at fungere godt eks. håndtering af sikkerhedsbrud og indsigtsanmodninger. Ligeledes blev uddannelsesindsatsen implementeret med succes. Der er dog forsat områder, hvor kommunen vil kunne få kritik ved et eventuelt kontrolbesøg fra Datatilsynet idet risikolandskabet løbende ændrer sig.

Det er ligeledes blevet mere tydeligt for Databeskyttelsesrådgiveren, at det er uklart, hvordan ansvarsfordelingen mellem mit, dit og vores ansvar udmøntes i operationelle handlinger i organisationen og hvor mange ressourcer der reelt anvendes på databeskyttelse i Københavns Kommune.

Den samlet vurdering er, at Københavns Kommune fik og stadig har et godt udgangspunkt i forhold til at efterleve de regler for behandling af personoplysninger, der er fastsat i Databeskyttelseslovgivningen. Det er dog også Databeskyttelsesrådgiverens vurdering, at der er forhold, der skal forbedres såfremt den nødvendige fremdrift i databeskyttelsen i Københavns Kommune skal sikres.

Der henvises til afsnit 4 Anbefalinger, for yderligere oplysninger herom.

2.2 Kulturen i Københavns Kommune i forhold til databeskyttelse

Indholdet i den nye databeskyttelseslovgivning er på visse områder en videreførelse af den tidligere persondatalov, som generelt ikke blev taget seriøst nok i kommunerne. Dette, sammenholdt med den nye lovgivnings omfattende krav til dokumentation af ansvarlighed, krav om en risikobaseret tilgang til foranstaltninger og øget fokus på opfyldelse af registreredes rettigheder har sammen med øget digitalisering medført et behov for en generel kulturændring i kommunerne i forhold til databeskyttelse.

Vi vurderer kulturen i forhold til hvordan de enkelte ledelseslag (beslutnings- og sagsforberedende kredse) tilgår arbejdet med databeskyttelse. Ligeledes indgår en vurdering af ledelsens opbakning til Databeskyttelsesrådgiveren og forvaltningernes indsats via Business Partnerne og Vejledende Sikkerhed i KIT- med hensyn til databeskyttelse.

Helt overordnet er det Databeskyttelsesrådgiverens vurdering, at alle ledelseslag i Københavns Kommune tidligt forstod vigtigheden og konsekvenserne af persondataforordningen.

Hele forløbet med etablering af Legal Compliance Projektet, udpegning af en Databeskyttelsesrådgiver og efterfølgende Business Partnerne i forvaltningerne og senest det besluttede omfattende regelsæt vedrørende databeskyttelse, understøtter og dokumenterer denne vurdering.

Forvaltningerne har via Business Partnerne og Vejledende Sikkerhed i KIT lagt mange ressourcer i at få understøttet forretningen i arbejdet med databeskyttelse – både i relation til rådgivning og uddannelse af ansatte i en bred opgaveportefølje samt rådgivning af borgere. Derudover spiller Business Partnerne en afgørende rolle i kommunens håndtering af sikkerheds- og persondatabrud.

Det er endvidere Databeskyttelsesrådgiverens vurdering, at der er den fornødne opbakning og forståelse for Databeskyttelsesrådgiverfunktionens rolle og ansvar.

Det at være rådgivende og kontrollerende i samme funktion er altid et dilemma. Databeskyttelsesrådgiveren må gerne opfattes som en ressource frem for en autoritet, selv om opgaverne også omfatter overvågning og tilsyn samt rapportering heraf til BR, ØU og forvaltningernes ledelse.

Vi er vidende om at Databeskyttelsesrådgiverens rolle og ansvar i flere større kommuner, giver anledning til udfordringer i det daglige arbejde med persondatabeskyttelse. Vi vurderer ikke, at det er tilfældet i Københavns Kommune og tilskriver dette to forhold. For det første er forvaltningerne i Københavns Kommune vant til at samarbejde med uafhængige funktioner idet Borgerrådgiveren og Intern Revision i forvejen fungerer i samme rolle. For det andet at Databeskyttelsesrådgiveren ligger i Intern Revision gør at kendskabet, mekanismerne og samarbejdet på forhånd var kendt af forvaltningerne.

Formelt formuleret er succeskriteriet for Databeskyttelsesrådgiveren i Københavns Kommune at understøtte ledelsen i at opnå de forretningsmæssige mål. Det gør vi bedst ved at blive inddraget tidligt i de forretningsmæssige processer, hvor behandling af persondata er en del af processen. I samarbejde med forvaltningerne kan vi identificere og rådgive om risici i forhold til persondatabeskyttelse og dermed proaktivt medvirke til, at processerne er designet, så de lever op til compliance og lovmæssige krav på persondataområdet.

2.3 Risikolandskabet i statusperioden

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 endvidere et krav, at de foranstaltninger, der skal sikre denne ansvarlighed, skal baseres på en risikovurdering. En risikovurdering skal identificere risikoen ***for at registreredes rettigheder og frihedsrettigheder bringes i fare*** *ved* en behandling af personoplysninger.

Et brud i forhold til fysiske personers rettigheder eller frihedsrettigheder kan indebære følgende konsekvenser:

"Fysisk, materiel eller immateriel skade – forskelsbehandling, identitetstyveri, identitetssvig, økonomiske konsekvenser/tab, skade på omdømme, sociale konsekvenser, indflydelse på privatliv, skade på menneskelig værdighed eller legitime interesser, begrænsning / krænkelse af fundamentale rettigheder og frihedsrettigheder, forhindring af udøvelse af kontrol med egne oplysninger".

Som dataansvarlig har Københavns Kommune igangsat og afsluttet flere initiativer for at reducere de overordnede risici:

- At kommunen ikke efterlever databeskyttelseslovgivningen
- At databeskyttelsen i kommunen ikke er betryggende

Ud fra det nuværende vidensniveau, er det Databeskyttelsesrådgiverens vurdering at kommunens indsatser i statusperioden har elimineret eller reduceret risikoen til lav eller middel på flere væsentlige aktivitetsområder. Der henvises til bilag 1 for yderligere information om Risikovurdering på indsatsområder i statusperioden.

2.3.1 Væsentlige ændringer i risikolandskabet

Risikolandskabet i forhold til databeskyttelse ændrer sig løbende. Det er således nødvendigt løbende at genbesøge risikolandskabet og minimum en gang årligt. Dette skyldes at nye vejledninger, fortolkninger og udmeldinger fra centrale myndigheder identificerer nye risici.

Københavns Kommune vurderes endvidere at være en stor og kompleks organisation i forhold til implementering af databeskyttelse. En effektiv implementering betyder, at regler og retningslinjer skal være kendte, accepterede og efterlevet i praksis i yderste led i organisationen og derfor vurderes størrelsen og kompleksiteten i kommunen som en risiko i sig selv.

Det er Databeskyttelsesrådgiverens vurdering, at der er sket væsentlige ændringer i risikolandskabet og der er identificeret flere nye aktivitetsområder, som vurderes at være højrisiko.

Højrisikoområder skal både medføre aktiviteter på tværs i kommunen og i de respektive forvaltninger. Risikolandskabet skal yderligere kvalificeres i et samarbejde mellem forvaltningerne, Databeskyttelsesrådgiveren og Vejledende sikkerhed i KIT. Herefter kan der foretages en koordineret indsats rettet mod disse.

3. VÆSENTLIGE SIKKERHEDSBRUD I STATUSPERIODEN

Persondatabrud håndteres af forvaltningernes Business Partnere og processen er beskrevet i en fælles administrativ forretningsgang. Forretningsgangen for persondatabrud er en nøgleproces som Databeskyttelsesrådgiveren løbende overvåger.

Økonomiforvaltningen fører en opgørelse over persondatabrud på tværs af kommunens forvaltninger og orienterer Økonomiudvalget to gange årligt.

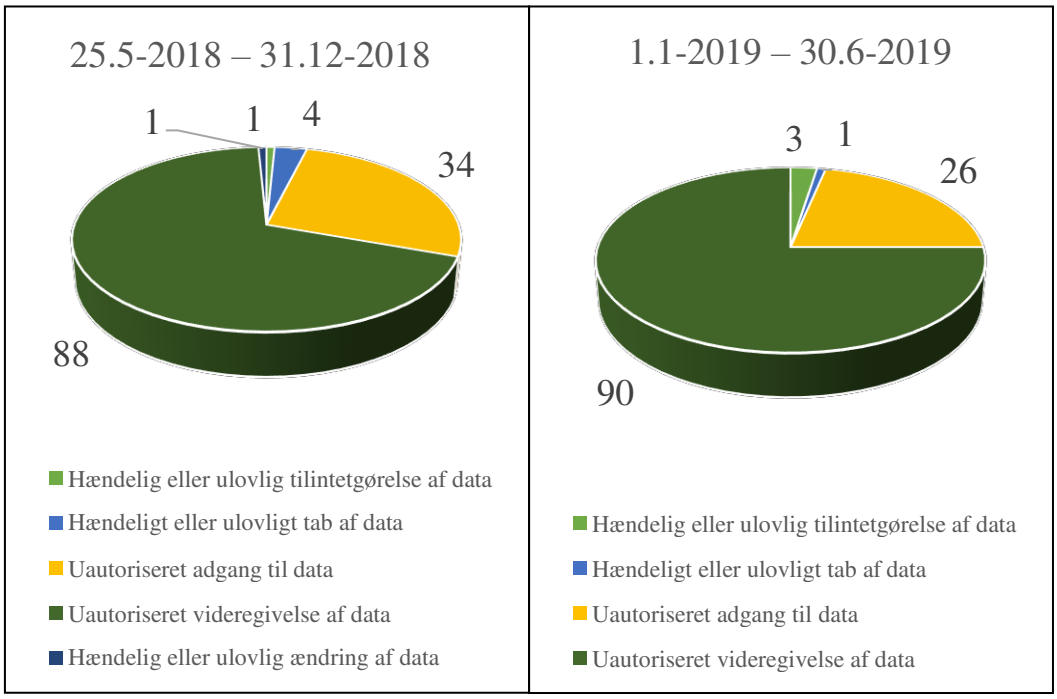
Antallet af brud på tværs af kommunens forvaltninger varierer en del. Alle brud registreres efter type. Typerne dækker over en uhensigtsmæssig omgang med data, der har medført:

- tilintetgørelse, f.eks. at data slettes i et it-system
- tab, f.eks. at data mistes ved tyveri
- videregivelse, f.eks. at data sendes til forkerte personer udenfor kommunen
- ændring, f.eks. at data redigeres fejlagtigt i en sagsakt
- adgang, f.eks. at data er blevet set af en uvedkommende sagsbehandler

Der er i perioden fra 25. maj 2018 til 30. juni 2019 registreret 248 brud i KK

	25.5-31.12.2019	Første halvår 2019
Konstaterede brud	128	120

Tabel 1: Antal af brud på persondatasikkerheden i 2018 og 2019



Figur 2: Persondatabrud fordelt på typer

Efter ikrafttrædelsen af Databeskyttelsesforordningen den. 25. maj 2018 skal Københavns Kommune (KK) anmelde brud på persondatasikkerheden (persondatabrud) til Datatilsynet medmindre, det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder. I perioden 25. maj 2018 til 30. juni 2019 er 145 brud blevet anmeldt til Datatilsynet.

Antallet af brud og anmeldelser viser en let stigende tendens i 2019 i forhold til 2018. I forhold til kommunens størrelse er andelen af persondatabrud, der anmeldes til Datatilsynet på samme niveau som gennemsnittet for landets kommuner. Om stigningen er et udtryk for flere brud eller et udtryk for, at kommunerne er blevet mere opmærksomme på at registrere og indberette brud, er uvist.

Hyppigste fejlkilder til brud i KK er utilsigtet videregivelse af data, hvilket følger tendensen på landsplan, hvor 2/3 del af brudene kan henføres til det at sende ukrypteret ("usikker mail") eller til "forkert" modtager.

4. ANBEFALINGER TIL HVORDAN EFTERLEVELSEN AF DATABESKYTTELSE FORBEDRES

Databeskyttelsesrådgiverens rolle og opgaver er fastsat i databeskyttelseslovgivningen med Justitsministeriets og Datatilsynets tilhørende Vejledninger. Databeskyttelsesrådgiveren er en i kommunen uafhængig funktion, der fungerer som kommunens rådgiver og tilsynsfunktion på området og skal inddrages og rådføres om overholdelse af de databeskyttelsesretlige regler.

En af de væsentligste opgaver for Databeskyttelsesrådgiveren er at overvåge overholdelsen af de databeskyttelsesretlige regler i kommunen. Det indebærer bl.a. at overvåge kommunens politikker om databeskyttelse, uddannelsen af personale i databeskyttelse, oplysningskampagner, fordeling af ansvar og revisioner etc.

Hvad er der behov for fremadrettet?
På baggrund af den løbende overvågning af budget, ledelsesopbakning, organisatoriske/tekniske foranstaltninger, kompetencer m.v. har Databeskyttelsesrådgiveren følgende anbefalinger:

- Det er vigtigt fortsat at have ledelsesmæssigt fokus på persondataretten i alle henseender. Det betyder b.la.:
    - At passe på borgernes og medarbejdernes data skal være en del af vores kultur
    - Uddannelse og oplysning er en vedvarende proces
    - Vi skal drage erfaringer fra de brud der sker ved at spotte trends og mindske risiko for gentagelser
    - Implementering af regler og retningslinjer er først effektiv når disse er kendte, accepterede og efterlevet i praksis i yderste led i organisationen
    - Vi skal koordinere indsatsen på tværs af hele kommunen
    - Tilpasninger i forhold til databeskyttelsesindsatsen skal løbende vurderes

Det kræver topledelsens fortsatte opbakning til indsats og udholdenhed.

4.1 Tilpasning af den nuværende databeskyttelsesindsats

1,5 år efter persondataforordningens ikrafttræden og arbejdet hermed har hele organisationen fået mere viden, indsigt og erfaringer med databeskyttelse. Som anført i afsnit 2 omkring et konstant ændret risikobillede som kræver hurtig beslutningsdygtighed og tværgående aktiviteter, er det Databeskyttelsesrådgiverens vurdering, at der er forhold der skal forbedres såfremt den nødvendige fremdrift i databeskyttelsen i Københavns Kommune skal sikres.

Overordnet er problemstillingen i forhold til arbejdet internt i Kommunen:

- Manglende koordinering af den samlede operationelle indsats
- Manglende overblik over udmøntningen/operationalisering af ansvarsområder
- Overblik over de ressourcer der anvendes samlet i Kommunen

Databeskyttelsesrådgiveren anbefaler derfor at der igangsættes et arbejde, der skal medvirke til, at der også fremadrettet ydes en omkostningseffektiv databeskyttelsesindsats i Københavns Kommune.

I arbejdet bør indgå at der:

- sikres overblik over de samlede ressourcer, der er til rådighed
- foretages en præcisering af roller og ansvarsområder
- foreligger koordinerede funktionsbeskrivelser
- foretages en samlet koordinering af indsatsen (årshjul) og udarbejdes årsplaner for indsatsen

Således sikres at de ressourcer der er til rådighed anvendes til en effektiv og koordineret indsats, som medvirker til reel fremdrift af databeskyttelsen i KK og at de tilførte midler anvendes bedst muligt.

5. SELVEJENDE INSTITUTIONER MED DRIFTSOVERENSKOMST

Borgerrepræsentationen har 11. oktober 2018 besluttet at give selvejende institutioner med driftsoverenskomst, muligheden for, at kommunens databeskyttelsesrådgiver vederlagsfrit varetager rollen som databeskyttelsesrådgiver.

Københavns Kommune har selvejende intuitioner i BUF, SOF og SUF-regi, og det at borgerne oplever en ensartet og betryggende håndtering af personoplysninger er væsentligt for kommunen.

Hvis institutionerne tager imod tilbuddet, gennemføres et Legal Complianceprojekt hos hver enkelt institution. Projektet skal medvirke til, at institutionen får kendskab til lovgivningen og overholder den i praksis i de daglige aktiviteter.

Ud af 237 selvejende institutioner har 202 institutioner takket ja til tilbuddet. Resultatet vurderes som yderst tilfredsstillende. De 35 institutioner, der har afslået tilbuddet, har typisk begrundet deres afslag med, at de har etableret en egen databeskyttelsesrådgiverfunktion.

De berørte forvaltninger har vurderet, at et eksternt Databeskyttelsesset-up umiddelbart er betryggende. Dog har forvaltningerne rettet henvendelse til

de ansvarlige ministerier med henblik på at undersøge kommunens muligheder for tilsyn hos disse institutioner. På baggrund af ministeriernes svar, er forvaltningerne ved at undersøge, hvad de konkrete muligheder for et tilsyn er, herunder hvilke rammer det evt. vil kunne udføres under.

Legal Complianceprojektet kører efter planen, og det forventes afsluttet med udgangen af januar 2020. Derefter vil kommunens databeskyttelsesrådgiver være institutionernes lovpligtige rådgiver, der medvirker til at fastholde og støtte op om alt indenfor databeskyttelsesområdet.

København, den 1. november 2019

Københavns Kommune Databeskyttelsesrådgiverfunktion

Jesper Gjøtterup Andersen
Databeskyttelsesrådgiver for Københavns Kommune

Nicholai Mandrup **Line Nymann Schoop** **Stine Thulin Everhøj**

Lone Forsberg **Christian Sonn Kjelmann**

BILAG 1 RISIKOVURDERING PÅ INDSATSOMRÅDER I STATUSPERIODEN

Risikolandskabet i statusperioden

Af databeskyttelseslovgivningen fremgår, at den dataansvarlige (Københavns Kommune), er forpligtiget til at foretage en risikovurdering af databeskyttelsen, når en behandling af personoplysninger sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder.

Som dataansvarlig har KK igangsat og afsluttet flere initiativer for at håndtere de væsentligste risici.

Oversigt over status på udrulning og efterlevelse af væsentlige aktiviteter i statusperioden

Aktivitet	Ansvarlig	Risiko klassifikation aktuel	Status på udrulning og efterlevelse (compliance niveau – se skala nedenfor)	Handlingsplaner	Afsluttet
Forretningscirkulærer vedrørende databeskyttelse	ØKF	Lav	Tilstrækkeligt designet	Afsluttet	2019
Cyber- sikkerhedsvurdering	ØKF	Mellem	Dokumenteret og kommunikeret	Afsluttet	2019
Risikovurdering af systemer	ØKF	Mellem	Dokumenteret og kommunikeret	Afsluttet	2019
Design og implementering af Uddannelseskoncept	Alle	Lav	Overvåget og vurderet	Afsluttet	2019
Udpegning af databeskyttelsesrådgiver	BR	Ingen	Overvåget og vurderet	Afsluttet	2018
Etablering af artikel 30 fortegnelse	Alle	Lav	Effektiv	Afsluttet	2018
Privatlivspolitik	Alle	Lav	Effektiv	Afsluttet	2018
Proces for indsigtsanmodninger	Alle	Lav	Effektiv	Afsluttet	2018
Proces for persondatabrud	Alle	Lav	Effektiv	Afsluttet	2018
Skabelon for databehandleraftaler	Alle	Lav	Effektiv	Afsluttet	2018
Identificere behandlingsprocesser med højrisiko	Alle	Lav	Effektiv	Afsluttet	2019
Udarbejdet data-databehandleraftaler	Alle	Lav	Effektiv	Afsluttet	2019

Skala for compliance niveau

Niveau	Definition	Forklaring
5	**Overvåget og vurderet**	Processen er tilstrækkeligt designet, effektivt efterlevet, overvåget og vurderet
4	**Effektiv**	Processen er tilstrækkeligt designet og effektivt efterlevet
3	**Tilstrækkeligt designet**	Processen er tilstrækkeligt designet, dokumenteret, men ikke effektivt efterlevet
2	**Dokumenteret og kommunikeret**	Processen er dokumenteret og kommunikeret, men ikke tilstrækkeligt designet
1	**Regelmæssigt mønster**	Processen proces følger et regelmæssigt mønster men er ikke dokumenteret
	Ad hoc eller ikke eksisterende	Proces eksisterer ikke