INTERN REVISION

STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

For perioden 1.oktober 2020 til 1.oktober 2021

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Indledning

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ udarbejder Databeskyttelsesrådgiveren årligt pr. 1. oktober en statusrapport. Rapporten indeholder en vurdering af databeskyttelsen i Københavns Kommune.

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

I lighed med tidligere år, er der kun udarbejdet en rapport for kommunen som helhed, hvilket vurderes at være mest hensigtsmæssigt. Fremover vil statusrapporten blive udarbejdet i overensstemmelse med Intern Revisions funktionsbeskrivelse.

2. Vurdering af databeskyttelsen i Københavns Kommune

2.1. Modenhedsvurdering

Databeskyttelsesrådgiveren har i 2021, etableret et grundlag for en modenhedsvurdering, som vil kunne 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.

Databeskyttelsesrådgiveren vil fremover rapportere på modenheden i den årlige statusrapport.

Modenhedsvurderingen scorer de enkelte forvaltninger og kommunen på udvalgte hovedområder og complianceområder indenfor databeskyttelse. Der scores fra 0 – 5 i spændet "væsentligt kritisk niveau" til "høj moden- og ansvarlighed".

Hypotesen er, at hvis der arbejdes bevidst med at forbedre modenheden, vil man, på et oplyst grundlag, kunne reducere risikoen til et acceptabelt niveau. Et mål om et modenhedsniveau i forvaltningerne i spændet mellem "Tilstrækkeligt" eller "Høj" bør tilstræbes.

Der er tale om "væsentligt kritisk", såfremt der er fuldstændigt fravær af politikker og processer og organisationen på ingen måde har erkendt behovet for struktureret styring og aktiviteter. Et "tilstrækkeligt modenhedsniveau" gives, når der er designet et regelsæt, som er implementeret og som til dels også virker effektivt, dog uden at der er nogen egentlig kontrol der kan dokumentere eller bekræfte effektiviteten.

I 72 ud af 92 complianceområder er vurderingen, at kommunen har et højt eller tilstrækkeligt modenhedsniveau, hvilket er meget positivt. 17 complianceområder ligger i kritiske niveauer.

> *I forhold til, at have passende regler og retningslinjer, har Københavns kommune generelt et højt eller tilstrækkeligt modenhedsniveau på databeskyttelsesområdet.*

At løfte niveauet på de kritiske 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 17 områder ud af de kritiske niveauer.

Det anbefales, at forvaltningerne anvender modenhedskonceptet som et ledelsesværktøj der sætter rammerne for arbejdet med databeskyttelse.

Såfremt anbefalingen følges, vil Databeskyttelsesrådgiveren introducere forvaltningerne og it-kredsen for konceptet.

Databeskyttelsesrådgiverens vil, som en del af overvågningsforpligtigelsen, løbende foretage tilsyn som skal validere forvaltningernes angivelse af modenhed.
Læs mere om modenhedsvurderingskonceptet under afsnit 3.

2.2. Efterlevelse af regler og retningslinjer

Databeskyttelsesrådgiveren har i 2021 foretaget tilsyn på to områder. Det ene var rettet mod forvaltningernes efterlevelse af fortegnelseskravet. Tilsynet viste, at forvaltningerne ikke har sikret, at regler og retningslinjer vedrørende fortegnelsen blev efterlevet.

Det andet tilsyn var rettet mod tre forvaltninger, for at påse efterlevelse af oplysningspligten. Tilsynet viste, at to af forvaltningerne, ikke i tilstrækkelig grad efterlever reglerne om oplysningspligt.

2021 har vist en nedadgående kurve i forhold til at efterleve regler og retningslinjer. Fortegnelseskravet og reglerne om oplysningspligt er essentielle områder, indenfor databeskyttelsesretten.

2.3. Risikovurdering

Databeskyttelsesrådgiveren har, på baggrund af indgående kendskab til både kommunen og forvaltningernes arbejde med databeskyttelse, foretaget en overordnet risikovurdering.

Det er vores vurdering, at de seks største risici i Københavns kommune, i ikke prioriteret rækkefølge, er:

	1 Compliance i forvaltningerne	2 Fortegnelsen	3 Risikovurdering af behandlingsprocesser
Risikobeskrivelse	Forvaltningerne skal, som en del af opgaven med at udvise ansvarlighed, sikre faste rammer for løbende overvågning af, at procedurer og retningslinjer er etableret og følges.	Fortegnelseskravet følger af databeskyttelsesforordningen. Fortegnelseskravet skal skabe gennemsigtighed og indblik i forvaltningernes mangeartede behandlinger af personoplysninger.	Risikovurderingerne er helt afgørende for at vurdere og fastsætte passende sikkerhedsforanstaltninger vedrørende behandlingsprocesser.
Risikovurdering	På nuværende tidspunkt har forvaltningerne ikke et styringsværktøj, som sikrer et overblik over hvilke regler og retningslinjer, der er udarbejdet, kommunikeret og hvorvidt de følges. Der er en væsentlig risiko for, at databeskyttelsesindsatsen bliver ustruktureret og personafhængig.	Vores tilsyn har vist, at forvaltningerne ikke løbende overvåger og ajourfører fortegnelserne. Således er der en væsentlig risiko for urigtige oplysninger og manglende gennemsigtighed, i forhold til de behandlinger forvaltningerne foretager.	Forvaltningerne foretager ikke de nødvendige risikovurderinger, og derfor kan forvaltningerne ikke dokumentere, at der træffes passende tekniske og organisatoriske sikkerhedsforanstaltninger.
Anbefalet handling	Forvaltningerne kan anvende modenhedskonceptet som et ledelsesværktøj, der sætter rammerne for arbejdet med databeskyttelse. Desuden er det aftalt med Økonomiforvaltningen, at der skal anskaffes et understøttende it-system i 2022, der skal medvirke til klare og ensartede processer på tværs af forvaltningerne på området.	Der bør udarbejdes en fællesadministrativ forretningsgang for håndtering af fortegnelseskravet i Københavns kommune. Forvaltningerne oplyser, at der vil ske en koordinering og fælles tilgang til risikoområdet som besluttes og implementeres i 2022.	Der bør udarbejdes en fællesadministrativ forretningsgang for håndtering af risikovurderinger i Københavns Kommune. Forvaltningerne oplyser, at der vil ske en koordinering og fælles tilgang til risikoområdet som besluttes og implementeres i 2022.

	4 Konsekvensanalyser	5 Tilsyn med databehandlere	6 Oplysningspligten
Risikobeskrivelse	Det er et grundlæggende krav i databeskyttelsesforordningen, at der udarbejdes konsekvensanalyser på alle behandlinger, der opfylder bestemte kriterier, eller hvor en risikovurdering viser høj risiko	Forvaltningerne har ansvaret for de personoplysninger, der behandles af en databehandler. For at kunne dokumentere dette ansvar og udvise ansvarlighed, kræves det, at der føres et dokumenteret tilsyn med eksterne databehandlere.	Det er et grundlæggende krav i databeskyttelsesforordningen, at forvaltningerne oplyser borgerne i tilstrækkeligt omfang, om de behandlinger deres personoplysninger benyttes i forbindelse med. Oplysningspligten skal understøtte gennemsigtigheden med de behandlinger, som kommunen foretager og give borgerne mulighed for at gøre brug af deres rettigheder.
Risikovurdering	Kommunens nuværende konsekvensanalyseværktøj er ikke tilstrækkeligt i forhold til de generelle krav, der anses at være til en konsekvensanalyse. Der er udarbejdet et nyt koncept, som vil blive implementeret i forbindelse med kommunens nye risikokoncept.	Forvaltningerne udfører ikke strukturerede tilsyn med databehandlere. Der er igangsat initiativer der skal sikre et løbende tilsyn ud fra et fast og ensartet tilsynskoncept på tværs af kommunen.	Vores tilsyn har vist, at to ud af tre forvaltninger ikke efterlever oplysningspligten, i tilstrækkelig grad.
Anbefalet handling	Det nye koncept for konsekvensanalyser bør indarbejdes i en fællesadministrativ forretningsgang. Som led i implementeringen af det nye risikovurderings-koncept, bør forvaltningerne vurdere, hvorvidt der skal udarbejdes konsekvens-analyser på allerede eksisterende behandlings-processer.	Det nye koncept for tilsyn med databehandlere bør indarbejdes i en fællesadministrativ forretningsgang. Forvaltningerne oplyser, at der vil ske en koordinering og fælles tilgang til risikoområdet som besluttes og implementeres i 2022.	Forvaltningerne bør gennemgå alle behandlinger med henblik på at sikre, at kravet om oplysningspligt efterleves i tilstrækkelig grad.

> *Det anbefales, at det i 2022 sikres, at forvaltningernes aktivitetsplaner omfatter en indsats som reducerer risikoen på de seks største risici, til et acceptabelt niveau.*

Generelt er kommunens regler og retningslinjer meget overordnede. Der er derfor i mange tilfælde behov for, at der udarbejdes fællesadministrative forretningsgange, der

koordineres og godkendes af IT-Kredsen (forvaltningernes it-direktører). Fællesadministrative forretningsgange medvirker til at sikre en ensartet tilgang til databeskyttelse på tværs af kommunen.

Vores tilsyn og risikovurdering jævnfør ovenfor viser, at der generelt er behov for en mere ensartet og driftsmæssig tilgang til databeskyttelsesområdet. I statusrapporterne for 2019 og 2020 pegede Databeskyttelsesrådgiveren på nogle konkrete forhold, der burde forbedres for at sikre den nødvendige fremdrift i databeskyttelsen i Københavns Kommune.

> *Det anbefales, at der i langt højre grad sikres ensartet administration på tværs af forvaltningerne ved udarbejdelse af fællesadministrative forretningsgange. Dette sikrer endvidere, at ressourcerne anvendes bedst muligt i forhold til at sikre den nødvendige databeskyttelse i Københavns Kommune.*

Et væsentligt initiativ, som i den forbindelse blev besluttet, var at Økonomiforvaltningen skulle sikre, at der blev udarbejdet et kommissorium for et GDPR koordinator-forum.

GDPR koordinator-forum skulle fremover, i tæt samarbejde med Databeskyttelsesrådgiveren, varetage koordineringen af databeskyttelsesindsatsen i kommunen, herunder koordinering af forvaltningernes aktivitetsplaner og årshjul samt prioritering, tilrettelæggelse og udførelse af tværgående complianceindsatser.

Vi kan konstatere, at Økonomiforvaltningen ikke er lykkedes med dette tiltag. Det er Databeskyttelsesrådgiverens vurdering, at alle forvaltninger bør opprioritere deres indsats generelt og i GDPR-forum, så anbefalingerne knyttet til risikoområderne implementeres hurtigt og ensartet på tværs af forvaltningerne. Som ansvarlig for GDPR-forum har Økonomiforvaltningen tilsluttet sig dette.

> *Det er vores vurdering, at forvaltningerne ved at følge de anbefalinger der er anført i vores risikovurdering, ved udgangen af 2022, vil kunne opnå et nødvendigt og væsentligt bedre complianceniveau på databeskyttelsesområdet.*

2.4. Schrems II

Tredjelandsoverførsler er et af de store emner inden for databeskyttelse i 2021. Den meget omtalte Schrems II-afgørelse, afsagt af EU-domstolen d. 16. juli 2020, medfører, at udveksling af personoplysninger mellem EU og USA ikke er muligt på baggrund af den hidtil gældende privacy-shield aftale.

Dommen slår fast, at USA - på grund af sine vidtgående rammer for statslig overvågning - ikke kan stille et niveau af databeskyttelse, der svarer til det, vi kender inden for EU med GDPR. EU-dommen betyder, at USA nu betegnes som et usikkert tredjeland.

Hvis man foretager en overførsel af personoplysninger til et "usikkert" tredjeland, skal man vurdere, hvorvidt landet har et tilstrækkeligt beskyttelsesniveau, svarende til det der er gældende indenfor EU/EØS.

Forvaltningerne har besluttet følgende:

- **Igangværende overførsler til usikre tredjelande**
  Vurderinger er igangsat i samarbejde mellem forvaltningerne og Databeskyttelsesrådgiveren.
- **Igangsættelse af nye overførsler, nye behandlinger, ændringer, eller udvidelser af eksisterende overførsler**
  KK påtager sig ikke yderligere risici ved at foretage ændringer, eller udvidelser, af eksisterende overførelser eller igangsætte nye behandlinger, der medfører en forøgelse af risikoen ved overførsel til usikre tredjelande.
- **Cloud-projektet**
  Projektet er på baggrund af de usikre forhold omkring cloud, sat på hold siden marts 2021. Koncern it og Databeskyttelsesrådgiveren følger løbende udviklingen, med henblik på at vurdere, om projektet kan genoptages.

Beslutningen følger Databeskyttelsesrådgiverens anbefaling.

> *EU-dommen udfordrer mange af kommunens nye tiltag på digitaliseringsområdet, som på nuværende tidspunkt ikke kan gennemføres, da leverandørerne ikke kan sikre et tilstrækkeligt beskyttelsesniveau. Selvom det er udfordrende på mange måder, skal der være tillid til, at Københavns Kommune som offentlig virksomhed kan passe på borgernes data.*

Databeskyttelsesrådgiveren følger udviklingen omkring Schrems II på tæt hold og holder kredsen af it-direktører opdateret, og vurderer løbende hvis der kommer ny viden.

Læs mere om Københavns Kommunes håndtering af Schrems II afgørelsen under afsnit 6.

2.5. Henvendelser til Databeskyttelsesrådgiveren

Databeskyttelsesrådgiveren ønsker at rådgive og vejlede forvaltningerne i videst muligt omfang. Statistikken viser, at der i det seneste år har været et aftagende behov fra forvaltningerne til at tage kontakt til Databeskyttelsesrådgiveren. Det er vores opfattelse, at forvaltningerne med fordel kan inddrage Databeskyttelsesrådgiveren mere i implementeringen af de forskellige værktøjer, der løbende udarbejdes.

Siden 1. oktober 2019 har Databeskyttelsesrådgiveren ført statistik over hvor mange henvendelser, der har været fra de enkelte forvaltninger. Henvendelserne giver Databeskyttelsesrådgiveren et indblik i, hvordan de databeskyttelsesretlige regler forvaltes og er med til at skabe opmærksomhed på tværgående problemstillinger samt give indblik i forvaltningsspecifikke udfordringer m.v.

En henvendelse bliver registreret, når Databeskyttelsesrådgiveren kontaktes for rådgivning og vejledning.

I perioden 1. oktober 2020 til 1. oktober 2021 har vi haft 116 henvendelser fra forvaltningerne.

3. Udført arbejde

Databeskyttelsesrådgiverens opgaver og aktiviteter er i overvejende grad fastlagt i de aktivitetsplaner, der er behandlet og godkendt af Revisionsudvalget.

3.1. Modenhedsvurderingskoncept

Databeskyttelsesrådgiveren har i 2021 etableret et grundlag for en modenhedsvurdering, som vil kunne 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.

Databeskyttelsesrådgiveren vil fremover rapportere på modenheden i den årlige statusrapport til Borgerrepræsentationen, Økonomiudvalget og forvaltningernes ledelse.

Modenhedskoncept er udarbejdet med afsæt i emner og kontroller fra ISO 27701, 27001 og 27002.

På nuværende tidspunkt er konceptet i stand til på overordnet niveau at illustrere, hvorvidt der i Københavns Kommune er udarbejdet regler og retningslinjer, som er styrende eller retningsvisende for forvaltningerne ift. databeskyttelse. I Københavns Kommune er det regler, som er defineret i forretningscirkulærer og fællesadministrative forretningsgange.

I løbet af 2022 vil vi udbrede konceptet til forvaltningerne, således at de ved at besvare de opstillede spørgsmål selvangiver sig ud fra bestemte parametre fastsat i konceptet. I forbindelse med næste statusrapport vil vi helt eller delvist kunne illustrere forvaltningernes individuelle modenhed i forhold til udarbejdelse af regler m.v., implementering heraf og til dels om reglerne efterleves i praksis.

Forvaltningernes modenhedsvurdering vil give et godt indblik i på hvilke områder, der er behov for tiltag i de enkelte forvaltninger. Det vil også give indblik i hvilke områder, der efter forvaltningernes egen vurdering er compliant med regler og retningslinjer, og dermed kan indgå i Databeskyttelsesrådgiverens tilsynsplan. Konceptets 21 hovedområder og 92 complianceområder danner fremadrettet rammerne for de emner, som Databeskyttelsesrådgiveren planlægger sine tilsyn ud fra, og det forvaltningerne vil blive målt på. Derfor inviteres forvaltningerne til at benytte modenhedskonceptet, som en fast del af deres compliance arbejde.

Konceptet består af 92 complianceområder, der f.eks. vedrører håndtering af databehandlertilsyn, udarbejdelse af risikovurderinger, håndtering af mobile devices, overførelser til tredjelande m.v.

De 92 complianceområder henhører alle under hver deres hovedområde. Et hovedområde er en henvisning til, hvad de underliggende complianceområder vedrører.

Et hovedområde kan f.eks. være "Medarbejdersikkerhed før, under og efter ansættelsen" eller " Mobilt udstyr og fjernarbejdspladser" og alle hovedområder har et ID.nr. som overskueliggøre rapporteringen.

Forvaltningernes selvangivne modenhed vil over tid 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 vurdering.

Konceptet måler modenhed på en skala fra 0-5.

Niveau	5	4	3	2	1	0
Definition	Høj moden- og ansvarlighed	Høj modenhed	Tilstrækkeligt modenhedsniveau	Umodent	Kritisk niveau	Væsentligt Kritisk niveau

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 af det enkelte complianceområde og fastsættes af Databeskyttelsesrådgiveren ud fra en objektiv vurdering og med afsæt i konceptets vurderingsprincipper.

På områder hvor forvaltningerne er umodne og dermed ikke klar til egentlige tilsyn, vil der være en periode, hvor forvaltningerne kan bringe området op til et forventet modenhedsniveau. Dette vil efterfølgende skulle afspejles i forvaltningernes aktivitetsplaner, så der ud fra en risikobaseret tilgang arbejdes med de enkelte udestående.

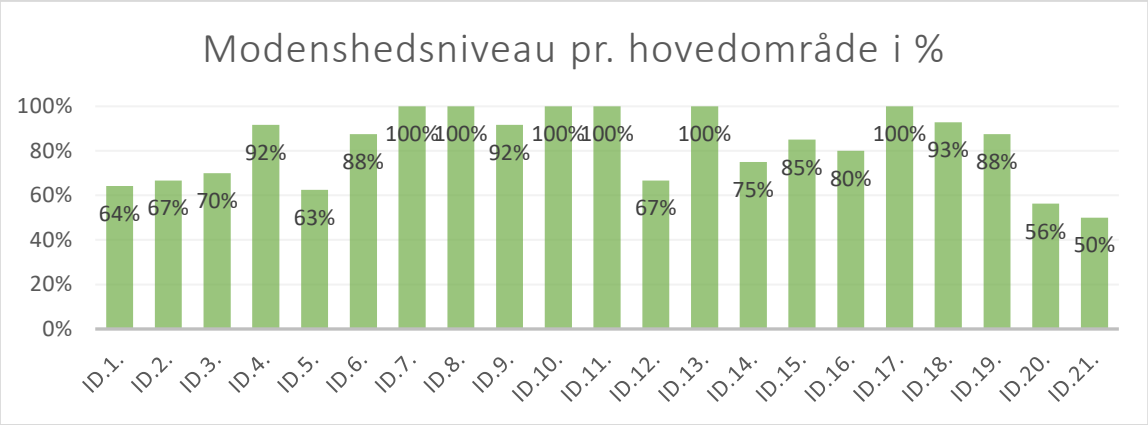
Konceptet vil kunne understøtte forvaltningernes fremadrettede arbejde ud fra en mere compliance -og risikobaseret tilgang ift. databeskyttelse. Konceptet vil ligeledes kunne understøtte forvaltningernes ledelsesrapportering, da det vil give et grundigt overblik over databeskyttelsesmodenheden år for år.

Konceptet vil løbende blive justeret, hvis der opdages uhensigtsmæssigheder eller andre forbedringspotentialer.

3.2. Vurdering af modenhed i Københavns Kommune

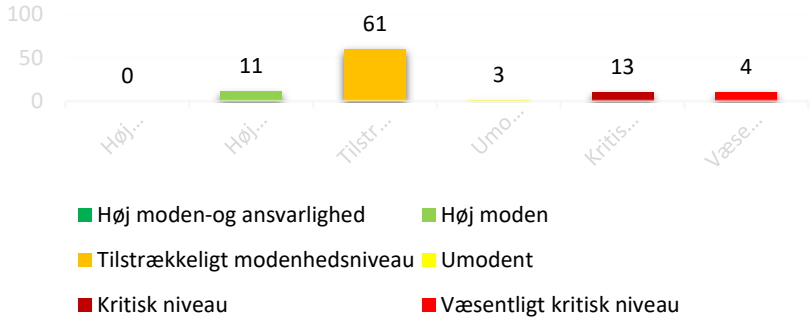
Som nævnt, er vurderingen i 2021 kun et udtryk for, hvorvidt Københavns Kommune på overordnet niveau har udarbejdet regler og retningslinjer, som er styrende eller retningsvisende for forvaltningerne ift. databeskyttelse.

Det vurderes, at Københavns Kommune i forhold til at have passende regler og retningslinjer, generelt har et højt eller tilstrækkeligt modenhedsniveau på databeskyttelsesområdet.



Som det fremgår, er det vurderingen, at Københavns Kommune på de fleste hovedområder er langt i arbejdet med at udarbejde regler og retningslinjer. Der er enkelte områder, hvor vi har identificeret mangler i kommunens overordnede regelsæt. For at sikre fortrolighed omkring modenhedsniveauets konkrete emner, er ID-numrene ikke nærmere angivet i forhold til emne.

Nedenstående tabel viser antallet af complianceområder, i forhold til modenhed på de enkelte complianceområder.



Grundet offentliggørelsen af Databeskyttelsesrådgiverens Statusrapport vil der ikke blive foretaget en yderligere uddybning af de enkelte områder.

3.3. Tilsyn med fortegnelse

Databeskyttelsesrådgiveren har i 2021 gennemført tilsyn med forvaltningernes efterlevelse af databeskyttelsesforordningens fortegnelseskrav. Det kunne konstateres, at forvaltningerne ikke havde sikret en tilstrækkelig governance i forhold til den løbende vedligeholdelse af deres fortegnelser siden implementeringsprojektet i 2018.

Siden databeskyttelsesforordningens ikrafttræden, er der ligeledes kommet nye retningslinjer fra Datatilsynet, som ikke var implementeret i nogen af forvaltningerne.

Det er dog Databeskyttelsesrådgiverens vurdering, at alle forvaltninger er opmærksomme på deres forpligtigelser.

Forvaltningerne er på nuværende tidspunkt i gang med at udarbejde nye fortegnelser, der sikrer overholdelse af gældende lovgivning samt de nye krav fra Datatilsynet.

Databeskyttelsesrådgiveren har planlagt at følge op på forvaltningernes handleplaner samt implementeringen i 2022.

Databeskyttelsesrådgiveren havde på baggrund af tilsynet en række anbefalinger.
Vi anbefalede at forvaltningerne:

- Udarbejder og implementerer en fælles obligatorisk forretningsgang for, hvordan arbejdet med løbende vedligeholdelse, kvalitetssikring, kontrol m.v. jf. forretningscirkulærer for dokumentation og compliance pkt. 1.1 & 2.1, håndteres inden udgangen af 2021. Processen for udarbejdelse og godkendelse af den fælles administrative forretningsgang skal følge Københavns Kommunes regelhierarki.
- Gør det til en fast aktivitet i forvaltningernes compliance årshjul for GDPR-koordinatorerne at foretage kontrol med rigtigheden af de oplysninger, der er anført i fortegnelsen.
- Fremadrettet finder en fælles løsning for, hvordan de yderligere indholdsmæssige krav til fortegnelsen fra Datatilsynet implementeres og håndteres.
- Finder en fælles løsning for, hvordan hjemmelsangivelsen skal anføres, når det vedrører behandling af personoplysninger af følsom karakter jf. artikel 9.
- Vurderer og eventuelt anskaffer et nyt system til håndteringen af fortegnelseskravet, hvis kravene fra Datatilsynet eller forvaltningernes behov har resulteret i, at den nuværende løsning ikke længere kan understøtte håndteringen af fortegnelseskravet.

Tilsynet gav anledning til anmærkning af væsentlig karakter.

3.4. Tilsyn med oplysningspligt

I 2021 blev der ligeledes gennemført et mindre tilsyn med tre af forvaltningernes håndtering af kravet om oplysningspligt, over for dem de behandler personoplysninger om. Oplysningspligten er en grundlæggende rettighed, som skal sikre grundlaget for gennemsigtigheden med de behandlinger, som kommunen foretager, således at borgerne kan benytte deres basale rettigheder, som fx er at foretage indsigelser mod behandlingen eller at anmode om sletning m.v.

Tilsynet blev foretaget med udgangspunkt i en stikprøvekontrol i forvaltningernes fortegnelse. Ud af de tre forvaltninger viste undersøgelsen, at der kun var én forvaltning der formåede at have grundlæggende styr på efterlevelsen af oplysningspligten over for de registrerede.
Hos de to øvrige forvaltninger har tilsynet givet anledning til anmærkninger af væsentlig karakter, idet forpligtigelsen i al væsentlighed ikke blev efterlevet.

Databeskyttelsesrådgiveren har planlagt en opfølgning ift. forvaltningernes handleplan samt implementeringen i 2022.

3.5. Tilsyn der ikke blev gennemført

I statusrapporten for 2020 havde Databeskyttelsesrådgiven meddelt, at der ville blive foretaget opfølgning for tilsynet med forvaltningernes uddannelsesplaner fra 2019, samt håndtering af persondatabrud.

Grundet Covid-19, samt andre udefra påvirkende omstændigheder, som fx Schrems afgørelsen, har Databeskyttelsesrådgiveren måtte udsætte disse tilsyn til 2022.

4. Afgørelser fra Datatilsynet

Databeskyttelsesrådgiveren orienterer årligt om væsentlige afgørelser og henvendelser fra Datatilsynet. Der henvises endvidere til afsnit 5, vedrørende sager om persondatabrud.

4.1. Manglende overholdelse af tidsfrisk for anmodning om indsigt

D. 2. februar 2021 udtalte Datatilsynet kritik af Københavns Kommune, fordi en indsigtsanmodning ikke var besvaret inden for tidsfristen på 30 dage jf. databeskyttelsesforordningens artikel 12, stk. 3.

4.2. Anvendelse af samme passwords til alle elever

Sagen er indledt på baggrund af en klage til Datatilsynet. Klager's henvendelse til Datatilsynet angik dels datterens brugernavn til Unilogin, som angiveligt var blevet videregivet til uvedkommende, og dels at passwordet ikke havde et tilstrækkeligt sikkerhedsniveau.

Datatilsynet fandt, at Københavns Kommune i perioden op til 18. februar 2020 ikke havde gennemført passende foranstaltninger for at sikre et passende sikkerhedsniveau, jf. databeskyttelsesforordningens artikel 32, stk. 1, og udtaler i den sammenhæng kritik af Københavns Kommune. Datatilsynet lagde vægt på, at samtlige elever i klagers datters klasse i perioden op til 18. februar 2020 anvendte samme password til at logge på hver deres computer, og det måtte derfor antages, at mange har været bekendt med passwordet, og at det af disse årsager har været let for uvedkommende at få adgang til elevernes oplysninger.

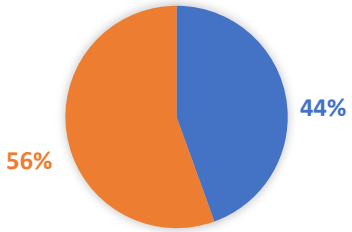
Datatilsynet finder ligeledes at Københavns Kommune ikke har levet op til kravet om anmeldelse af brud på persondatasikkerheden jf. databeskyttelsesforordningens art. 33, stk.1.

5. Persondatabrud

Det er Databeskyttelsesrådgiverens opfattelse, at forvaltningerne har en god proces for håndteringen og koordineringen af persondatabrud, at medarbejderne har en god forståelse for, hvad et persondatabrud er og har evnen til at identificere hændelser.

Databeskyttelsesrådgiveren oplever forsat, at antallet af brud på tværs af kommunens forvaltninger varierer en del.
I perioden 1. oktober 2020 til den 1. oktober 2021 er der blevet registeret 466 persondatabrud i Københavns Kommune.

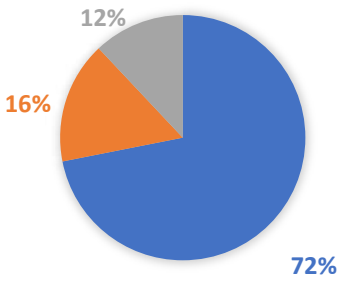
Figur 1. Sager der har været anmeldt til Datatilsynet i det tilfælde sagen har haft karakter af et persondatabrud:



Viser antal sager (206) hvor forvaltningen har vurderet, at der ikke har været behov for at anmelde sagen til Datatilsynet.

Viser antal sager (165) 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 (56), som endnu ikke er afsluttet.

Viser antal sager (335), hvor forvaltningerne har vurderet, at der var tale om et persondatabrud.

Viser antal sager (75), 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 vil i 2022 se på håndteringen af persondatabrud.

Databeskyttelsesrådgiveren har kendskab til, at Københavns Kommune i alt har modtaget 177 afsluttende breve fra Datatilsynet for indberettede persondatabrud i perioden 1. oktober 2020 til 1. oktober 2021.

I 174 af sagerne har der ikke været anledning til udtalelse fra Datatilsynet. I tre sager har Københavns Kommune modtaget et påbud, en udtalelse med kritik samt en udtalelse med alvorlig kritik.

5.1. Sager, hvor Københavns Kommune har modtaget påbud fra Datatilsynet

En ekstern leverandør havde ikke formået at inddrage en fratrådt medarbejders systemadgang. Efter fratrædelsen har medarbejderen haft kontakt med flere af kommunens borgere, som var tilknyttet en beskæftigelsesindsats hos leverandøren. Datatilsynet nedlagde **påbud** om, at Københavns Kommune skulle underrette alle registrerede, som havde været berørt af bruddet, da kommunen på tidspunktet for anmeldelsen endnu ikke havde taget stilling. Forvaltningen har efterfølgende underrettet 33 borgere.

5.2. Sager, hvor Københavns Kommune har modtaget alvorlig kritik fra Datatilsynet

Sagen er indledt på baggrund af en klage indgivet til Datatilsynet.

I forbindelse med en flytteanmeldelse videregav Kultur-og Fritidsforvaltningen en tidligere ægtefælles nye adresse, som var underlagt adressebeskyttelse.
Datatilsynet har i sagen lagt vægt på, at Københavns Kommune ikke har udført passende kvalitetskontrol af indholdet af det fremsendte brev, og dermed utilsigtet har videregivet oplysninger om klager til uvedkommende. Herudover har tilsynet lagt vægt på, at brevet indeholdt oplysninger om klagers beskyttede adresse, og at denne oplysning blev videregivet til en person, som klager havde et konfliktfyldt forhold til.
Sagen gav anledning til, at Datatilsynet har indskærpet, at Københavns Kommune fremover anmelder lignende sikkerhedsbrud til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1.

Samlet set var der således grundlag for at udtale **alvorlig kritik** af kommunen, idet behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1 og artikel 33, stk. 1.

5.3. Sager, hvor Københavns Kommune har modtaget kritik fra Datatilsynet

Grundet en teknisk fejl har Socialforvaltningen videregivet en borgers beskyttede adresse til dennes tidligere samlever. Baggrunden for fejlen var en manglende opdatering af borgerens

stamdata. Derfor var vedkommendes tidligere samlever forsat registeret med C/O navn på borgerens adresse, ligesom den tidligere samlever var registreret som primær kontakt, på trods af, at borgeren i mellemtiden var flyttet og havde fået beskyttet adresse.

Datatilsynet fandt grundlag for at udtale **kritik** af kommunen, da forvaltningen ikke i tilstrækkeligt omfang havde sikret sig, at de behandlede oplysninger var korrekte. Derved havde kommunen ikke havde truffet passende organisatoriske og tekniske foranstaltninger for at sikre rigtigheden af de behandlede oplysninger, jf. databeskyttelsesforordningens artikel 32, stk. 1, og artikel 5, stk. 1, litra d.

Socialforvaltningen modtog yderligere kritik, da forvaltningen ikke havde anmeldt bruddet uden unødig forsinkelse, jf. databeskyttelsesforordningens artikel 33, stk. 1.

6. Schrems II

Tredjelandsoverførsler har været et af de store emner inden for databeskyttelse i 2021. Den meget omtalte Schrems II-afgørelse, afsagt af EU-domstolen d. 16. juli 2020, medfører, at udveksling af personoplysninger mellem EU og USA, ikke er muligt på baggrund af den hidtil gældende privacy-shield aftale.

Dommen slår fast, at USA, på grund af sine vidtgående rammer for statslig overvågning, ikke kan stille et niveau af databeskyttelse, der svarer til det vi kender inden for EU med GDPR. Den beskyttelse, som personoplysninger nyder inden for EU, skal følge personoplysningerne, uanset hvor i verden de befinder sig. Grundtesen er, at borgerne ikke skal have forringet deres databeskyttelse, blot fordi kommunen vælger en leverandør til at bistå os med fx et system.

EU-dommen betyder, at USA nu betegnes som et usikkert tredjeland.

Kommunen skal derfor selvstændigt foretage en vurdering af modtagerlandets lovgivning, for at fastlægge om de europæiske garantier for databeskyttelse er de samme, som dem der følger af GDPR. Det er netop denne vurdering, som EU-domstolen har foretaget af USA's lovgivning, og domstolen er kommet frem til, at niveauet af databeskyttelse og rettigheder for de registrerede for USA's vedkommende, ikke lever op til niveauet af beskyttelse som følger af GDPR.

Amerikansk lovgivning tillader deres efterretningstjenester, disproportionalt, at indsamle personoplysninger fra amerikanske selskaber og datterselskaber, også selvom datterselskabet har hovedsæde i EU. Dette desuagtet at personoplysningerne er "kommunens" samt at virksomhedens infrastruktur eller serverer eventuelt står i EU. Lovgivningen er ligeledes skruet sådan sammen, at kommunen aldrig ville kunne blive oplyst om, hvorvidt personoplysningerne var blevet givet til en efterretningstjeneste fordi virksomhederne underlægges tavshedspligt.

Databeskyttelsesrådgiveren er af den opfattelse, at problematikken i Københavns Kommune kan inddeles i 3 grupper, og har anbefalet følgende:

- Igangværende overførsler til usikre tredjelande
  Der udarbejdes Transfer impact assessments jævnfør henstillingerne fra Datatilsynet. Koncern it og Databeskyttelsesrådgiveren tilrettelægger en proces i overensstemmelse med drøftelserne i IT-kredsen. Forvaltningerne bør afvente denne proces.

- Igangsættelse af nye overførsler, nye behandlinger, ændringer, eller udvidelser af eksisterende overførsler
  Københavns Kommune bør ikke påtage sig yderligere risici ved foretage ændringer eller udvidelser af eksisterende overførelser eller igangsætte nye behandlinger, der medfører en forøgelse af risikoen ved overførsel til usikre tredjelande. Det er Databeskyttelsesrådgiverens opfattelse, at det vil være uansvarligt, såfremt forvaltningerne bevidst øger risikoen ved yderligere overførsel eller behandling i

usikre tredjelande. Det henstilles, at forvaltningerne samt Koncern it inddrager eller orienterer Databeskyttelsesrådgiveren såfremt forvaltningerne mod forventning øger kommunens risiko i forbindelse med overførsel til tredjelande.

- <u>Københavns kommunes Cloudprojekt</u>
  Cloudprojektet er ganske fornuftigt sat på hold, indtil videre.

Hvis man foretager en overførelse til et "usikkert" tredjeland, skal man vurdere, hvorvidt landet har et tilstrækkeligt beskyttelsesniveau, som det der er gældende indenfor EU/EØS. Denne undersøgelse kaldes en TIA (transfer impact assessment), som må anses for at være en omfattende undersøgelse, som skal danne grundlaget for, om en overførsel kan igangsættes eller fastholdes.

Databeskyttelsesrådgiveren vurderer, at der er to muligheder, hvor minimum én skal være opfyldt, før en overførsel til et usikkert tredjeland kan ske. Disse er følgende:

- Man kan på baggrund af en omfattende sandsynlighedsvurdering redegøre for, hvorfor eventuelt problematisk lovgivning ikke har praktisk betydning ift. den behandling, som man ønsker at igangsætte.

- Der skal være truffet tilstrækkelige supplerende foranstaltninger.

En sandsynlighedsvurdering anses for at være meget omfattende, og kræver en udførlig dokumentation på baggrund af objektive kriterier og pålidelige kilder. Vurderingen må således ikke udelukkende baseres på kommunens egen vurdering eller en leverandørs vurdering.

Supplerende foranstaltninger betyder, at man forsøger at afhjælpe eventuelle utilstrækkeligheder i beskyttelsesniveauet i et usikkert tredjeland. Det kan være tekniske, organisatoriske eller kontraktuelle foranstaltninger, der højner databeskyttelsesniveauet til det der er gældende indenfor EU/EØS. Dette gælder f.eks. hvis man har leverandører fra USA. Det er vigtigt at pointere, at foranstaltningerne skal være effektive i praksis og ikke blot på papiret.

Københavns Kommune har udarbejdet en forretningsgang for håndtering af Schrems II, hvor både Koncern IT og Databeskyttelsesrådgiveren bliver inddraget i vurderingen af, om en overførsel kan ske. Databeskyttelsesrådgiveren vurderer alle sager ud fra et objektivt grundlag:

- Overføres der personoplysninger?
- Hvorvidt der er udarbejdet en sandsynlighedsvurdering eller
- Om der er truffet tilstrækkelige supplerende foranstaltninger.

Databeskyttelsesrådgiveren følger udviklingen omkring Schrems II på tæt hold.

7. Selvejende institutioner med driftsoverenskomst

Databeskyttelsesrådgiveren for de selvejende institutioner (DPOSI) er pr. 1. oktober 2021 DPO for 151 selvejende institutioner mod 153 institutioner pr. 1. oktober 2020.

De 151 institutioner er fordelt på 113 daginstitutioner, 14 sociale institutioner og 24 plejehjem.

Ca. 25% af institutionerne har i løbet af året henvendt sig med spørgsmål til GDPR og 12 institutioner har søgt hjælp til håndtering af databrud.

Den primære aktivitet i 2021 har været en screening af complianceniveauet hos samtlige selvejende institutioner gennem en spørgeskemaundersøgelse. Resultatet fra undersøgelsen er anvendt til at identificere institutioner med overvejende manglende compliance indenfor de adspurgte områder. Som følge deraf er der gennemført detaljeret tilsyn på 11 institutioner med efterfølgende rapport og rådgivning til ledelsen og bestyrelsen. De øvrige 140 institutioner har alle modtaget specifik vejledning og rådgivning indenfor de områder, hvor de ikke var compliant.

Vi har i 2021 desuden fokuseret på at gennemgå 438 databehandleraftaler, der er indgået med 51 databehandlere, som institutionerne anvender. Arbejdet skal blandt andet tjene som grundlag for en konkret indsats rettet mod databehandleraftaler i 2022.

23. september 2021 afholdte DPOSI en GDPR-netværksdag, hvor alle 151 institutioner var indbudt. 70 institutioner valgte at deltage i arrangementet, der havde til formål at drøfte GDPR-udfordringer i dagligdagen og udveksle løsninger, gode ideer og erfaringer. Netværksdagen var en stor succes med en ivrig dialog blandt deltagerne. Deltagerne bekræftede, at institutionerne føler sig trykke med DPOSI som en tilgængelig og effektiv rådgiver.

Det er vores opfattelse, at institutionerne generelt er motiveret og gør en indsats for at sikre korrekt håndtering og tilstrækkelig beskyttelse af personoplysninger, om end GDPR-ekspertisen stadig skal forbedres mange steder.

Desuden er der fortsat institutioner, der af forskellige årsager ikke har den basale GDPR på plads. Vi er meget opmærksomme på disse institutioner, og vil også i 2022 løbende rette henvendelse til lederne for at forbedre niveauet. Dette er også baggrunden for, at vi sideløbende med de kunderettede aktiviteter har brugt 2021 på at implementere et nyt GDPR-system. Systemet skal understøtte DPO-arbejdet, herunder synliggøre complianceniveau og aktiviteter hos hver institution, og vil i 2022 også kunne beregne institutionernes GDPR-risiko.

København, den 10. december 2021

Jesper Gjøtterup Andersen Databeskyttelsesrådgiver

Københavns Kommune Databeskyttelsesrådgiverfunktion

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