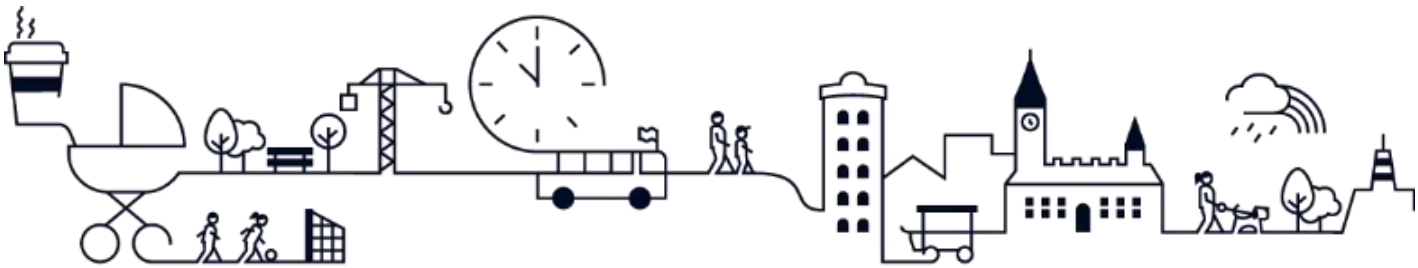
INTERN REVISION



STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

- Københavns Kommune

For perioden 1.oktober 2021 til 1.oktober 2022

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Indledning 3
2. Databeskyttelsesrådgiverfunktionen i Københavns Kommune 3
3. Status 4
5. Rådgivning, tilsyn og overvågning 8
6. Afgørelser fra Datatilsynet 9
7. Persondatabrud 10
8. Opfølgning på indsatsområder 2021 11
9. Databeskyttelsesrådgiverfunktionen for selvejende institutioner med driftsoverenskomst 14

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 indeholder en samlet vurdering af databeskyttelsen samt øvrige relevante forhold i relation til databeskyttelse i Københavns Kommune.

Der er endvidere udarbejdet en delrapport pr. forvaltning, som omfatter en vurdering af modenheden og de væsentligste risici på databeskyttelsesområdet i hver forvaltning.

Samlerapporten og de syv delrapporter fremsendes til forvaltningernes direktioner, til Revisionsudvalget og til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

2. Databeskyttelsesrådgiverfunktionen i Københavns Kommune

Borgerrepræsentationen har besluttet, at chefen for Intern Revision er kommunens Databeskyttelsesrådgiver, jf. § 26, stk. 3, i Styrelsesvedtægten for Københavns Kommune.

Databeskyttelsesrådgiverens opgaver er fastlagt i lovgivningen om databeskyttelse samt i Københavns Kommunes Informationssikkerhedsregulativ.

Forvaltningerne, de selvejende institutioner og borgere kan søge generel rådgivning vedrørende databeskyttelse hos databeskyttelsesrådgiverfunktionen, ligesom funktionen proaktivt yder konkret rådgivning overfor forvaltninger og selvejende institutioner.

Databeskyttelsesrådgiveren skal inddrages forud for udstedelse af retningslinjer og procedurer for, hvordan de databeskyttelsesretlige regler skal overholdes i kommunen, herunder informationssikkerhedspolitik, -regulativ, forretningscirkulærer, processer og forretningsgange mv.

Databeskyttelsesrådgiverens anbefalinger og rådgivning skal tages til efterretning af de respektive organisationer. Såfremt Databeskyttelsesrådgiverens anbefalinger og rådgivning ikke følges, skal dette dokumenteres i overensstemmelse med Databeskyttelsesforordningens krav om ansvarlighed.

Databeskyttelsesrådgiveren kan ikke gøres ansvarlig for kommunens eller de selvejende institutioners manglede overholdelse af gældende lovgivning. Overholdelse af de til enhver tid gældende databeskyttelsesretlige regler er til enhver tid kommunens eller institutionens ansvar.

3. Status

Snart fem år efter vi fik det nye GDPR-regelsæt er mange stadig usikre på, hvordan lovkravene skal fortolkes.

Nye afgørelser og fortolkninger, drevet af myndigheder, aktivister og privatpersoner betyder, at GDPR er et komplekst fagområde, man er tvunget til at følge tæt.

At målbillederne løbende ændrer sig, gør opgaven med databeskyttelse betydelig vanskeligere, og det stiller store krav til organisationen at sikre rette kvalitet og ensartethed i kommunen.

Det er derfor vigtigt, at der er klarhed over, hvem der rådgiver i forhold til fortolkninger, og hvad der reelt skal til for at efterleve kommunens regler og retningslinjer.

Databeskyttelsesrådgiverfunktionens opgave er at medvirke til at sikre et passende databeskyttelsesniveau i kommunen.

Ved at rådgive forvaltningerne om deres forpligtigelser i henhold til databeskyttelsesforordningen, anden EU-ret samt nationale bestemmelser på det databeskyttelsesretlige område, kan vi bedst medvirke til, at organisationen fremover kan håndtere compliance-arbejdet så smidigt og effektivt som muligt.

Derfor er der efter vores opfattelse behov for at få etableret en governance, som skaber klarhed over, hvordan vi løser de databeskyttelsesretlige opgaver bedst muligt med fokus på at gøre tingene ensartet, højne niveauet samt løse opgaverne på en mere omkostningseffektiv måde.

Anbefalingen understøttes yderligere af, at forvaltningerne er udfordret på fremdrift i forhold til de almindelige driftsopgaver, ligesom der er udfordringer angående koordinering af indsatser på tværs. Dette medfører mange spildte ressourcer og ikke i alle tilfælde den ønskede kvalitet i databeskyttelsesindsatsen.

I de efterfølgende afsnit har vi givet en status på konkrete emner, som vi skønner, kan være af betydning for Borgerrepræsentationen ved bedømmelsen af databeskyttelsen i Københavns Kommune.

Implementering af regler og retningslinjer

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.

Det er vores mål, at konceptet løbende vedligeholdes i et tæt samarbejde med forvaltningerne, som en del af at dokumentere det arbejde (ledelsestilsyn), der er udført. Hypotesen er, at hvis der arbejdes bevidst med at forbedre modenheden, vil man på et oplyst grundlag kunne reducere risikoen til et acceptabelt niveau.

Det er positivt, at alle forvaltningerne i 2022 har medvirket til at justere konceptet og foretage en selvangivelse i forhold til forvaltningens modenhed på 46 complianceområder.

Implementeringen af regler og retningslinjer vedrørende fortegnelse, risikovurderinger samt konsekvensanalyser pågår p.t.

Sidste år anførte vi, at indsatsen var for nedadgående. I år begynder vi igen at se fremgang.

Det har dog vist sig, at det er vanskeligt at nå til enighed om, hvilken kvalitet der er nødvendig, for at kunne leve op til kommunens regler og retningslinjer og dermed de databeskyttelseskrav, der er krævet i lovgivningen.

Det må være et fælles mål at få udarbejdet fortegnelser, risikovurderinger og konsekvensanalyser, som alle kan forklare og forsvare, når det bliver nødvendigt.

Schrems

Schrems problematikken har fyldt meget i de senere år, og i lighed med alle andre håber kommunen på en ny transatlantiskdataaftale mellem EU og USA, som kan løse udfordringerne ved at bruge cloudtjenester fra amerikanske virksomheder.

I lyset af Schrems II dommen blev det hurtigt besluttet, at kommunen ikke igangsatte nye behandlinger, udvidede eksisterende eller fortsatte sin planlagte cloudtransformation.

I Københavns Kommune er man i gang med at udarbejde egentlige exit-strategier frem mod december måned 2022, hvor der skal være fundet et nyt overførelsesgrundlag i takt med, at Europa-Kommissionens standardkontraktbestemmelser skal være opdateret.

Københavns Kommune har et stort antal systemer, hvor der er identificeret en problematik ift. overførsler til usikre tredjelande.

I oktober 2022 udstedte USA et længe ventet dekret, som skal danne grundlag for en ny aftale, der skal sikre, at persondata kan overføres frit og sikkert mellem EU og amerikanske virksomheder. Dekretet opstiller formålsbegrænsninger for amerikansk masseovervågning, og der introduceres proportionalitetsbetragtninger.

Desuden introduceres der en to-trins klagemodel, hvor europæiske borgere kan klage til en europæisk myndighed, der via en amerikansk instans kan indbringe sagen for en ny domstol, Data Protection Review Court.

Nu kan Europa-Kommissionen begynde at arbejde på en tilstrækkelighedsvurdering af USA, som måske resulterer i, at USA igen kan erklæres for et sikkert tredjeland.

På nuværende tidspunkt er det for tidligt for kommunen at ændre tilgangen til brug af cloudtjenester fra amerikanske virksomheder.

Det næste store spørgsmål er så, om den nye aftale, som, hvis den kommer, forventes at foreligge i marts 2023, bliver tilstrækkelig, eller om den vil blive udfordret ved EU-Domstolen, og om vi får en Schrems III sag.

Vi oplever til stadighed, at både større og mindre leverandører men også den offentlige sektor, bevidst negligerer problemstillingen, trækker tiden og udelukkende satser på en ny aftale med USA.

Hvis ikke der kommer en ny transatlantisk dataaftale med USA, risikerer kommunen i 2023 at stå i samme fastlåste situation som den nuværende og derved være udfordret i forhold til den fremtidige digitalisering og effektivisering af kommunen.

Chromebook

En sag mellem Helsingør Kommune og Datatilsynet, som rækker tilbage til 2019, har fyldt en del i den offentlige debat. Den 14. juli 2022 udstedte Datatilsynet et regulært forbud mod, at kommunen måtte bruge Chromebook-styresystemet og programmet Google Workspace i undervisningen, på skolerne i Helsingør Kommune.

Afgørelsens væsentligste elementer omhandler to forhold:

- Risikoen for, at Google anvender skoleelevernes data til andre formål, end kommuner har hjemmel til i folkeskoleloven.
- Udfordringerne ved, at Google, jf. databehandleraftalen med Helsingør kan overføre data til USA i forbindelse med support.

Selvom afgørelsen konkret forholder sig til behandlingen af personoplysninger i Helsingør Kommune, har det været Datatilsynets klare opfordring, at andre kommuner med tilsvarende forhold ser på de samme områder.

I Københavns Kommune har man medio 2022 sikret sig, at ingen Københavnske skoler anvender Google Workspace i undervisningen.

Det er dog ikke en ukendt problemstilling i Københavns Kommune, at leverandører anvender data til andre formål, end kommunen har hjemmel til samt foretager overførsler til usikre tredjelande, hvorfor kommunen også vil komme til at arbejde med denne problemstilling i 2023.

Efter Datatilsynets afgørelse om forbud mod brug af Google Workspace, har Kommunernes Landsforening, på vegne af landets øvrige kommuner, der oplever samme problemstilling som Helsingør Kommune, oprettet en arbejdsgruppe, som skal gå i dialog med Google. Kommunernes Landsforening vil derfor arbejde på at få justeret Googles løsning, så eleverne og lærernes personoplysninger kan behandles i overensstemmelse med databeskyttelsesforordningen.

Senest har Datatilsynet den 8. september 2022 foretaget en midlertidig suspension af forbuddet og har givet Helsingør Kommune fire påbud, som skal lovliggøre brugen af programmet. Såfremt Helsingør Kommune inden den 5. november 2022 kan dokumentere, at de efterlever de betingelser som Datatilsynet har stillet, kan Helsingør Kommune anvende Google Workspace på lovlig vis, og Datatilsynet kan endeligt hæve forbuddet. Idet Datatilsynet og KL ikke har udtalt sig offentligt om sagens omstændigheder efter den 5. november 2022, kan vi ikke give yderligere oplysninger i sagen.

Servicebesøg decentrale enheder i KK

Som led i Databeskyttelsesrådgiverens rådgivnings- og overvågningsforpligtelse, har vi i år foretaget en række servicebesøg hos udvalgte decentrale enheder i Børne- og Ungdomsforvaltningen og Socialforvaltningen.

Formålene med servicebesøgene har været at yde konkret rådgivning om behandling af personoplysninger i forbindelse med varetagelsen af enhedens kerneopgaver.

I 2022 er der foretaget i alt ti servicebesøg. I Børne- og Ungdomsforvaltningen har vi besøgt to daginstitutioner og én skole, og i Socialforvaltningen har vi besøgt syv bo- og dagtilbud.

Det er vores indtryk, at enhederne har fået afklaring på spørgsmål, som relaterer sig til deres daglige håndtering af personoplysninger, og at de besøgte enheder har en god forståelse for vigtigheden af, at beskytte de registreredes personoplysninger, samt at de tillige har et ønske om at efterleve lovgivningen.

En af de observationer, som går igen på servicebesøgene, har været uklarheder omkring anvendelse og deling af billeder/videoer, herunder i hvilket omfang enhederne må anvende og dele billeder af borgere. Herudover har spørgsmål vedrørende anvendelse af SMS-korrespondance med borgere, samt opbevaring af fysiske og elektroniske dokumenter indeholdende personoplysninger været drøftet.

Vi oplever en tendens til, at enheder fravælger en behandling af borgernes personoplysninger, i frygt for at databeskyttelsesretlige regler ikke overholdes. Ofte er der tale om fejlfortolkninger af lovgivningen, som ender ud i GDPR-myter, der desværre resulterer i benspænd for den enkelte medarbejder i deres hverdag. I samarbejde med enhederne har vi fundet frem til, at behandlingen af personoplysninger godt kan lade sig gøre, inden for lovens rammer.

Det er Databeskyttelsesrådgiverens samlede vurdering, at servicebesøgene har stor værdi for enhederne, og at der på længere sigt vil blive skabt en gennemgående og ensartet forståelse af databeskyttelsesreglerne på tværs af enhederne. Det er Databeskyttelsesrådgiverens hensigt at foretage flere servicebesøg hos nye enheder i 2023.

4. Igangværende tilsyn fra Datatilsynet

I Københavns Kommune er der på nuværende tidspunkt tre aktive tilsyn fra Datatilsynet.

Arkivloven

Det ene tilsyn vedrører kommunens administration af arkivlovens § 34.

I henhold til bestemmelsen kræver det i bestemte situationer samtykke fra Datatilsynet, hvis kommunen ønsker at få tilladelse til at benytte allerede arkiverede personoplysninger, samt når en person anmoder om indsigt i allerede arkiverede personoplysninger om vedkommende selv.

Tilsynet var et skriftligt tilsyn og blev indledt da Datatilsynet, efter en gennemgang af indkomne anmodninger om samtykke efter arkivlovens § 34, har kunnet konstatere, at Københavns Kommune kun har anmodet Datatilsynet om samtykke få eller ingen gange, inden for de seneste to år.

Tilsynet blev indledt den 5. juli 2022.

AULA

Det andet tilsyn vedrører Københavns Kommunes efterlevelse af databeskyttelsesforordningen, særligt med fokus på de tekniske og organisatoriske foranstaltninger, der er iagttaget for at leve op til kravet om et passende sikkerhedsniveau for kommunens behandlinger i AULA.

Tilsynet var ligeledes et skriftligt tilsyn, hvor kommunen senest den 10. august 2022 har besvaret spørgsmål fra Datatilsynet. Datatilsynet har bl.a. fået udleveret

- De risikovurderinger der ligger til grund for vurderingen af hvilken sikkerhed, der er anset passende for behandlinger af oplysninger om fysiske personer i "AULA", samt en beskrivelse af de generelle sikkerhedsmodeller i applikationen.
- I det omfang der er udarbejdet konsekvensanalyser, kopier af alle versioner af disse.
- En gennemgang af overvejelser om brugen af databeskyttelsesforordningens art. 25, i forbindelse med anskaffelsen og udviklingen af "AULA".
- En gennemgang af autorisations- samt adgangsstyringsmodeller.

Tilsynet blev indledt den 15. oktober 2021

Tv-overvågning

Det tredje tilsyn vedrører kommunens brug af tv-overvågning på en sikret døgninstitution for børn og unge. Tilsynet blev gennemført som et fysisk besøg. Tilsynet havde bl.a. fokus på kommunes efterlevelse af reglerne om oplysningspligt, formål med tv-overvågning, udlevering af tv-overvågning, opbevaringsfrister, indsigt m.v.

Tilsynet blev gennemført den 24. november 2022.

5. Rådgivning, tilsyn og overvågning

Databeskyttelsesrådgiverens opgaver er i overvejende grad fastlagt i en aktivitetsplan, der er behandlet og godkendt af Revisionsudvalget. Nedenfor gives en gennemgang af de sager der har fyldt mest ift. rådgivning og de tilsyn der er gennemført i 2022.

Rådgivning

Det seneste år har i væsentligt omfang været præget af tredjelandsoverførsler grundet Schrems II dommen. Store dele af Databeskyttelsesrådgiverfunktionens tid er derfor gået med rådgivning inden for dette område.

Rådgivningen består primært i at gennemgå de tekniske foranstaltninger i diverse løsninger for at vurdere, om den lever op til reglerne, samt at hjælpe med at fortolke leverandørens tilbagemeldinger til forvaltningerne. Vi har over hele perioden været involveret i omkring 50 konkrete sager.

Herudover har vi ydet rådgivning og bistand vedrørende følgende større indsatsområder:

- Databeskyttelsesrådgiveren indgår som observatør i Koncern IT´s arbejde med et styrket ledelsessystem for informationssikkerhed baseret på ISO 27001 ISMS (Information Security Management System.
- Løbende rådgivning, sparring og kvalitetssikring til forvaltningerne i forbindelse med deres arbejde med fortegnelser, risikovurderinger, samt konsekvensanalyser.
- I samarbejde med Koncern IT yde rådgivning i forbindelse med kommunens TIA projekt. Projektets formål er at gennemgå kontraktgrundlaget i forvaltningernes databehandleraftaler for at fastslå, hvorvidt der sker overførsel til USA. Herefter skal forvaltningerne enten se, hvorvidt tredjelandsoverførslerne kan håndteres, eller om der skal udarbejdes en exit-strategi i forhold til de enkelte systemer.

Tilsyn og overvågning

Databeskyttelsesrådgiveren har i år afsluttet tilsyn på databeskyttelsesområdet vedrørende anvendelse af kommunens Databank, håndtering af databrud og håndtering af indsigtsanmodninger.

Databank

> *"KK Databank er et fælles data storage kombineret med en række com-pute tools til analyse, machine learning og traditionel BI."*

KK Databank skal betragtes som et dataopbevarings-"system". Databanken kan således trække personoplysninger fra et forvaltningsspecifikt eller tværgående system fx Kvantum, hvorefter data kan anvendes til andre formål fx ledelsesstatistik, beregning af sandsynligheden for uddannelsesfrafald m.v.

Systemer eller databaser (som databanken), der muliggør samkøring og datalagring, har umiddelbart en høj iboende risiko i forhold til overholdelse af de databeskyttelsesretslige regler og dermed en høj risiko for de registrerede (borgerne). Det stiller store krav til velbeskrevne forretningsgange, identifikation af risici og etablering af kontroller, der skal sikre overholdelse af de databeskyttelsesretlige regler.

Tilsynet viste, at kommunens regler på området ikke blev efterlevet. Konklusioner og anbefalinger er meddelt Økonomiforvaltningen i en rapport.

Håndtering af persondatabrud

Formålet med tilsynet har været at påse, hvorvidt forvaltningerne efterlever den fællesadministrative forretningsgang for håndtering af persondatabrud.

Tilsynet har omfattet stikprøvekontrol, hos alle kommunens forvaltninger. Stikprøverne har haft fokus på:

- Om der foreligger en risikovurdering i de situationer, hvor der ikke er sket anmeldelse til Datatilsynet.
- Om fristen for anmeldelse, inden 72-timer er efterlevet i de situationer, hvor der er sket anmeldelse til Datatilsynet
- Om der foreligger en risikovurdering i de situationer, hvor der er sket anmeldelse til Datatilsynet men ikke underretning til borgeren(ne).
- Om underretningerne til borgerne har opfyldt mindstekravene.

Tilsynet viste, at forvaltningerne i al væsentlighed følger kommunens fællesadministrative forretningsgang. Der er dog behov for at revidere forretningsgangen, som ikke har været revideret siden 2018, ligesom forvaltningerne i forbindelse med eventuel underretning af borgerne skal benytte den udarbejdede skabelon.

Konklusion og anbefalinger er meddelt Økonomiforvaltningen og forvaltningernes GDPR-koordinatorer.

Tværgående processer for håndtering af indsigtsanmodninger

Databeskyttelsesrådgiveren igangsatte i 2022 et tilsyn med den tværgående proces for håndtering af indsigtsanmodninger.

Økonomiforvaltningen meddelte efterfølgende, at de agtede at revidere den nuværende forretningsgang for håndtering af tværgående indsigtsanmodninger jævnfør den Fællesadministrativ Forretningsgang for Persondatabeskyttelse - Registreredes Rettigheder.

Databeskyttelsesrådgiveren har derfor valgt at udsætte tilsynet, og har i stedet givet forvaltningen vores anbefalinger til ændringer i forretningsgangen.

6. Afgørelser fra Datatilsynet

Databeskyttelsesrådgiveren orienterer årligt om væsentlige afgørelser og henvendelser fra Datatilsynet. I 2022 har Københavns Kommune modtaget to afgørelser med kritik samt én afgørelse, der gav kommunen medhold i kommunens håndtering af telefoniske opkald.

Manglende indsigt

Datatilsynet fandt grundlag for at udtale kritik af, at Københavns Kommunes håndtering af klagers indsigtsanmodning ikke var sket i overensstemmelse med databeskyttelsesforordningens regler. Kommunen havde af flere omgange meddelt, at borgeren havde fået fuld indsigt i behandling af vedkommendes oplysninger.

Efter Datatilsynets involvering måtte forvaltningen hele to gange korrigere deres tidligere udmelding, da der blev fundet personoplysninger om klager, som ikke var blevet fundet første gang.

Sagen understreger vigtigheden af, at alle personoplysninger bliver behørigt journaliseret, samt at der er en stringent proces for, hvordan man gennemgår sine systemer for personoplysninger.

Manglende sletning

Datatilsynet fandt grundlag for at udtale kritik af, at Københavns Kommunes håndtering af klagers sletningsanmodning ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningen.

Klager kunne på baggrund af en indledende indsigtsanmodning konstatere, at kommunen behandlede oplysninger om vedkommende tilbage fra 2005. På den baggrund rettede klager henvendelse til Københavns Kommune og anmodede om, i videst muligt omfang, at få slettet oplysninger registreret om denne. Konkret ønskede klager at få slettet oplysninger registreret om ham fra 2000 til 2015, som han ikke længere anså for at have nogen relevans.

Personoplysninger om klager blev behandlet i fem forskellige forvaltninger, hvor vedkommende har haft konkrete sager.

Hver enkelt forvaltning har derfor været inde og forholde sig til, hvorvidt de har kunne efterkomme klagers sletteanmodning ift. den mængde oplysninger, de hver især har behandlet. De afgørelser som hver forvaltning kom frem til, fandt Datatilsynet ikke anledning til at påtale yderligere.

Kritikken bliver givet, idet Københavns Kommune ikke har overholdt de gældende tidsfrister for håndteringen af indsigtsanmodninger jf. Databeskyttelsesforordningen artikel 12, stk. 3.

Behandling af personoplysninger i forbindelse med telefoniske opkald til forvaltningen

Datatilsynet har på baggrund af en klage valgt at undersøge Københavns Kommunes behandling af personoplysninger i forbindelse med telefoniske opkald til Kultur- og Fritidsforvaltningen og eventuelt andre forvaltninger i kommunen.

Efter en gennemgang af sagen fandt Datatilsynet, at Københavns Kommunes behandling af personoplysninger er sket indenfor rammerne af databeskyttelsesforordningen.

Datatilsynet henstillede dog, at Københavns Kommune, hvis ikke kommunen i forvejen har indrettet sig på en sådan vis, udover at give borgeren oplysning om, at samtalen optages, også informerer om formålet med behandlingen af personoplysninger og henviser til et link på kommunens hjemmeside, hvor borgeren kan finde yderligere information om kommunens behandling af personoplysninger i forbindelse med opkald.

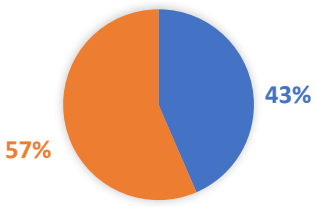
7. Persondatabrud

Det er vores vurdering, at medarbejderne generelt har en god forståelse af, hvad et persondatabrud er, samt har evnen til at identificere hændelser som leder til et persondatabrud.

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

I perioden 1. oktober 2021 til den 1. oktober 2022 er der blevet registreret 404 persondatabrud i Københavns Kommune. Sidste år, var dette tal 466.

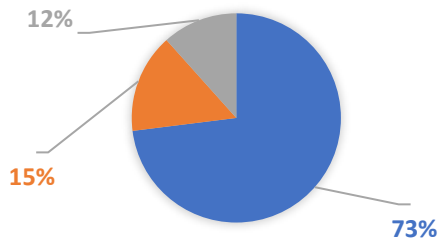
Figur 1. Sager der har været anmeldt til Datatilsynet i det tilfælde sagen har haft karakter af et persondatabrud:



Viser antal sager (191), hvor forvaltningen har vurderet, at der ikke har været behov for at anmelde sagen til Datatilsynet. Sidste år var tallet 206.

Viser antal sager (147), hvor forvaltningen har vurderet, at sagen skal anmeldes til Datatilsynet. Sidste år var tallet 165.

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



Viser antal sager (47), som endnu ikke er afsluttet.

Viser antal sager (295), hvor forvaltningerne har vurderet, at der var tale om et persondatabrud.

Viser antal sager (62), 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.

I 2022 har kommunen ikke modtaget nogen former for kritik i forhold til de indmeldte persondatabrud Datatilsynet har afsluttet.

8. Opfølgning på indsatsområder 2021

I Årsrapporten for 2021 anførte vi, at der var mangler i forhold til at efterleve og sikre en vedvarende databeskyttelsesindsats i forvaltningerne. Vi pegede på seks essentielle områder, hvor det er vigtigt, at forvaltningerne hurtigst muligt får sikret, at de databeskyttelsesretlige krav efterleves.

Det blev aftalt, at medio 2023 var en rimelig frist for forvaltningerne, i forhold til at færdiggøre fortegnelser, udarbejde risikovurderinger af behandlingsprocesser samt at udarbejde eventuelle konsekvensanalyser.

	Observation	Anbefaling	Status 2022
Compliance i forvaltningerne	På nuværende tidspunkt har forvaltningerne ikke et styringsværktøj, som sikrer et overblik over, hvilke regler og retningslinjer der er udarbejdet, er kommunikeret og hvorvidt de følges. Der er en væsentlig risiko for, at databeskyttelsesindsatsen bliver ustruktureret og personafhængig.	Forvaltningerne kan anvende modenhedskonceptet som et ledelsesværktøj, der sætter rammerne for arbejdet med databeskyttelse.	Alle forvaltningerne har i 2022 medvirket til at justere konceptet og foretaget en selvangivelse i forhold til forvaltningens modenhed på 46 complianceområder. Frist: Implementeret.

Fortegnelsen	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.	Der bør udarbejdes en fællesadministrativ forretningsgang for håndtering af fortegnelseskravet i Københavns kommune.	Økonomiforvaltningen har udarbejdet en fællesadministrativ forretningsgang for fortegnelser, og der er nu en ensartet rammesætning ift. kommunens håndtering af fortegnelseskravet. Alle forvaltningerne har igangsat arbejdet. Frist 31-12-2022.
Risikovurderinger	Forvaltningerne foretager ikke de nødvendige risikovurderinger af behandlingsprocesser, og derfor kan forvaltningerne ikke dokumentere, at der træffes passende tekniske og organisatoriske sikkerhedsforanstaltninger.	Der bør udarbejdes en fællesadministrativ forretningsgang for håndtering af risikovurderinger i Københavns Kommune.	Der pågår et arbejde omkring kommunens risikovurderingskoncept, som forventes afsluttet primo 2023.
Konsekvensanalyser	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.	Det nye koncept for konsekvensanalyser bør indarbejdes i en fællesadministrativ forretningsgang.	Konceptet er blevet implementeret, men er endnu ikke understøttet af en fællesadministrativ forretningsgang. Økonomiforvaltningen forventer, at denne vil være udarbejdet Q4 2022. Forvaltningerne er kun i meget lille omfang påbegyndt implementeringen.
Tilsyn med databehandlere	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.	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.	Der er endnu ikke udarbejdet en fællesadministrativ forretningsgang. ØKF har primo december fremsendt et udkast til fællesadministrativ forretningsgang for tilsyn med databehandlere, til kommentering hos Databeskyttelsesrådgiveren. Der er enkelte forvaltninger, der har meddelt, at de trods manglende forretningsgang er gået i gang med opgaven. Frist 30-6-2023.
Oplysningspligten	Vores tilsyn i 2020 viste, at to ud af tre forvaltninger ikke efterlever oplysningspligten, i tilstrækkelig grad.	Forvaltningerne bør gennemgå alle behandlinger med henblik på at sikre, at kravet om oplysningspligt efterleves i tilstrækkelig grad.	Forvaltningerne er i proces. Der er enkelte forvaltninger, der har meddelt, at de er færdige med arbejdet. Frist 31-12-2022.

Modenhed

I løbet af året har vi i samarbejde med forvaltningerne udarbejdet modenhedsvurderinger. Resultatet heraf fremgår af de forvaltningsspecifikke statusrapporter. Alle rapporter er understøttet af forvaltningernes selvangivelser. Forvaltningernes indledende vurdering indikerer, at de i al væsentlighed har sikret understøttelsen af deres databeskyttelsesindsats.

Databeskyttelsesrådgiveren vil validere forvaltningernes selvangivelser i takt med, at der føres tilsyn med de enkelte complianceområder.

Fortegnelse, risikovurdering og konsekvensanalyse

Som det fremgår af ovenstående, er der ligeledes udarbejdet og vedtaget fælles koncepter for udarbejdelse af fortegnelser. Alle forvaltningerne er i gang med at udarbejde fortegnelser i overensstemmelse med de vedtagne regler. Idet forvaltningernes risikovurderinger og eventuelle konsekvensanalyser er tæt knyttet til arbejdet omkring fortegnelserne, er der kun enkelte forvaltninger, der er påbegyndt dette arbejde.

Såfremt det skal være realistisk at overholde fristen medio 2023, er det vores vurdering, at der for hver forvaltning senest 31/12-2022, bør være udarbejdet en fuldstændig og kvalitetssikret fortegnelse. Vi er i løbende dialog med forvaltningerne omkring fortegnelsen og vil primo 2023 følge op på fremdriften i samarbejde med forvaltningernes ledelse.

Tilsyn med databehandlere

Kommunen har tilmeldt sig Det fælleskommunale Databehandlersekretariat (DBS), som omfatter ca. 60 kommuner.

Formålet med DBS er at sikre en ensartet praksis og at styrke kompetencerne på det kommunale databehandleområde samt at sikre en bedre forhandlingsposition for medlemskommunerne.

Konkret indebærer det, at foreningen skal bistå medlemskommunerne med:

- Tilsyn og kontrol med de databehandleraftaler, som medlemskommunerne har indgået med leverandører og samarbejdspartnere.
- Forhandling af databehandleraftaler på vegne af medlemskommunerne, herunder risikovurderinger af de databehandlinger, som aftalerne vedrører.

Ovenstående er under forudsætning af, at mindst 20 medlemskommuner har aftale med samme leverandør/samarbejdspartner.

Kommunen 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, har 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 kommunen. Herefter bør der foretages en koordinering, der sikrer mod overlap imellem forvaltningernes tilsyn og vedtages en fælles obligatorisk forretningsgang for tilsyn med databehandlere i kommunen, forinden tilsyn igangsættes.

Oplysningspligt

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

9. Databeskyttelsesrådgiverfunktionen for selvejende institutioner med driftsoverenskomst

Borgerrepræsentationen vedtog 11. oktober 2018, at der skulle fremsættes et tilbud til kommunens selvejende institutioner med driftsoverenskomst om vederlagsfrit, at få kommunens databeskyttelsesrådgiver som institutionens databeskyttelsesrådgiver.

Databeskyttelsesrådgiveren er pr. 1. oktober 2022 DPO for 145 selvejende institutioner. De 145 institutioner er fordelt på 111 daginstitutioner, 10 sociale institutioner og 24 plejehjem.

Den primære aktivitet i 2022 har været indsamling af informationer om, hvilke foranstaltninger den enkelte institution har truffet, for at sikre korrekt behandling og optimal beskyttelse af personoplysninger.

Resultatet af undersøgelsen er anvendt til at udregne og præsentere institutionerne for deres individuelle GDPR-risikoprofil. Profilen viser institutionens modenhed og evne til, gennem forskellige organisatoriske foranstaltninger, at imødekomme mulige risici for, at den registreredes rettigheder bringes i fare.

Profilen har givet institutionerne detaljerede informationer om, hvor deres risici er højst. Dermed har institutionerne fået en bedre mulighed for at iværksætte nødvendige forbedringsaktiviteter på de områder, der er mest relevante for den enkelte. I forlængelse af undersøgelsen har vi arbejdet fokuseret på at rådgive institutioner med høj risikoprofil.

Af væsentlige øvrige aktiviteter kan vi nævne:

- Håndtering af 144 opgaver, der har berørt 74 af institutionerne. Indeholdt heri er 7 institutioner, der har søgt hjælp til håndtering af databrud. Desuden har 10 institutioner fået ny leder, som har medført et genbesøg af institutionernes forståelse og complianceniveau samt en særlig rådgivning af de nye ledere, der som oftest ikke har fået overdraget GDPR-opgaven og viden om GDPR.
- Udvikling af en GDPR-folder til institutionernes medarbejder og en folder rettet mod institutionernes bestyrelser. Begge foldere giver anbefalinger til håndtering og beskyttelse af personoplysninger.
- Undervisning af institutionernes ledere og GDPR-ansvarlige ved flere virtuelle Åbent-Hus-arrangementer.
- Udviklet undervisningsmaterialer i form af videopræsentationer indenfor væsentlige GDPR-emner.

Det er vores samlede opfattelse, at institutionerne stadig gør en god indsats for at sikre korrekt håndtering og tilstrækkelig beskyttelse af personoplysninger. Vi har derfor også fastholdt rådgivning som den primære tilgang for at understøtte institutionerne.

Institutioner uden for ordningen

Ikke alle selvejende institutioner har valgt at være omfattet DPO-ordningen. For disse institutioner har forvaltningerne et eget ansvar for at påse at disse, i lighed med de øvrige institutioner i kommunen, opfylder databeskyttelseslovgivningens krav, og at håndtering og beskyttelsen af borgernes personoplysninger er ensartet.

Af de 28 institutioner som har valgt ikke at være omfattet DPO-ordningen kan én henføres til SUF, fire kan henføres til SOF og 23 henføres til BUF.

SOF har fire selvejende institutioner, hvor driftsoverenskomsten skal genforhandles. Det forventes, at institutionerne ved en genforhandling modtager tilbud om at tilslutte sig DPO-ordningen.

SUF har i 2022 påset, at det pågældende plejehjem har en navngiven ekstern DPO, samt at DPO-en har udarbejdet en årsrapport for 2022, hvor det vurderes at plejehjemmet generelt har et tilstrækkeligt GDPR-complianceniveau.

BUF har med rådgivning fra DPO for selvejende institutioner gennemført en undersøgelse på de 23 institutioner, der har valgt ikke at være omfattet DPO-ordningen. Institutionerne er anmodet om at besvare en række spørgsmål om deres complianceniveau med henblik på at vurdere umiddelbare risici for de registrerede (borgere og medarbejdere). Forvaltningen vil på baggrund af disse tilbagemeldinger at foretage en opfølgning med henblik på at vurdere videre tiltag.

Vi anbefaler, at forvaltningerne fortsat er proaktive i forhold til at få alle de selvejende institutioner med driftsoverenskomst, tilmeldt ordningen.

København, den 9. december 2022

Københavns Kommune Databeskyttelsesrådgiverfunktion

Jesper Gjøtterup Andersen

Databeskyttelsesrådgiver for Københavns Kommune

Nicholai Mandrup	Line Nymann Schoop	Christian Cramer Kjelmann
Lone Forsberg	Jonathan Brix	Luna Stenberg Lind
Anders Ettrup Gutfelt		