INTERN REVISION

STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

København Kommune

For året 2024

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Om Databeskyttelsesrådgiverens statusrapport

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance, udarbejder Databeskyttelsesrådgiveren (herefter omtalt som "vi") årligt en statusrapport.

Denne rapport indeholder en samlet status samt øvrige relevante forhold i relation til databeskyttelse i Københavns Kommune (KK).

Der er desuden udarbejdet en delrapport pr. forvaltning, som omhandler konkrete forvaltningsspecifikke forhold.

Samlerapporten og de syv delrapporter fremsendes til direktionen i de respektive forvaltninger, til Revisionsudvalget og til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

2. Sammenfatning

Fremskridt i arbejdet med databeskyttelse

2024 har været et vigtigt år for Københavns Kommunes arbejde med databeskyttelse. Forvaltningernes modenhed i at håndtere GDPR-krav er steget betydeligt, hvilket vidner om en fælles indsats og et stærkere fundament for at sikre overholdelsen af reglerne. Fremdriften har været særlig tydelig i arbejdet med at implementere flere af de grundlæggende GDPR-områder hvor forvaltningerne enten er, eller tæt på at være i mål med implementeringen.

I takt med denne udvikling har vi i det forløbne år prioriteret både rådgivning og tilsyn for at støtte forvaltningerne bedst muligt.

Fra 2025 vil vi dog ændre vores tilgang. Frem for at fokusere på et højt antal tilsyn vil vi styrke vores rådgivningsfunktion. Denne ændring skal sikre, at forvaltningerne får målrettet rådgivning til at opretholde en stærk GDPR-compliance, samtidig med at vi forebygger databrud og sikrer borgernes rettigheder.

Kunstig intelligens og databeskyttelse

Udviklingen af kunstig intelligens (KI) har spillet en stigende rolle i forvaltningerne i år og vi forventer, at ny teknologi i høj grad vil præge fremtiden.

Vi oplever i høj grad at forvaltningernes GDPR-funktioner involverer os tidligt i KI-projekter, hvor der sker behandling af personoplysninger, hvilket giver os mulighed for at være en aktiv sparringspartner i disse projekter.

Selvom KI åbner nye muligheder, vil den fremtidige implementering være afhængig af, om de regulatoriske krav kan opfyldes. Derfor forventer vi også at udbredelsen af løsninger, der behandler personoplysninger, vil ske langsomt på grund af juridiske udfordringer (lovhjemmel).

Rådgivning og tilsyn

I 2024 har vores rådgivningsindsats inkluderet både generelle anbefalinger og konkret rådgivning. Vi har set en stigning i antallet af borgere, der ønsker vejledning om deres rettigheder i forhold til GDPR. Vi har haft en god dialog med både borgere og forvaltninger, når det gælder besvarelse af spørgsmål og håndtering af klager.

Samtidig har vi intensiveret indsatsen med servicebesøg på decentrale enheder og udført tilsyn med fortegnelser, databehandleraftaler og sletning i eDoc.

Endelig har vi varetaget rollen som Databeskyttelsesrådgiver for 146 selvejende institutioner, der har driftsoverenskomst med Københavns Kommune.

Fremadrettet fokus

Denne rapport giver et samlet overblik over årets resultater og udfordringer, herunder indsatsen på tværs af forvaltningerne og arbejdet med specifikke fokusområder som kunstig intelligens, risikovurderinger og konsekvensanalyser m.v.

Vi håber, at rapporten vil give en god og brugbar indsigt i status for databeskyttelsesarbejdet og det arbejde, der ligger foran os.

3. Kunstig intelligens (KI-løsninger)

Tidligt i 2024 udarbejdede vi et notat til forvaltningerne hvor vi beskrev hvilke juridiske overvejelser der bør foretages, inden man påbegynder behandling af personoplysninger i en KI-løsning.

Datatilsynet har ligeledes været meget aktive i deres rådgivning omkring rammerne for brug af kunstig intelligens i den offentlige sektor, hvilket vi følger nøje.
Herudover deltager vi i en række KI-netværk, for at sikre, at vi har den nyeste viden inden for området, så vi kan rådgive forvaltningerne bedst muligt.

Sammen med SUF har vi deltaget i Datatilsynets regulatoriske sandkasse for KI, hvor SUF deltager med projektet "TALT".

Formålet med "TALT"-projektet er at lette dokumentationsbyrden for medarbejdere i sundheds- og omsorgsplejen. Løsningen skal gøre det muligt for medarbejdere at indtale dokumentation i journalen, få genereret sammenfattede versioner af journalen samt medvirke til, at dokumentation bliver korrekt journaliseret. Projektet "TALT" er fortsat i proces omkring de regulatoriske udfordringer.

Vi oplever også flere KI-projekter vedrørende muligheden for brug af KI til generering af et sagsresume. Vi er i dialog med flere forvaltninger om mulighederne indenfor deres respektive fagområder.

Det er nemt at se fordele ved den nye teknologi og selv om der er regulatoriske udfordringer, forventer vi at KI i endnu større grad vil præge 2025. Det må dog også forventes, at udbredelsen blandt offentlige myndigheder vil være en forholdsvis langsomlig proces, hvis der skal behandles personoplysninger, da der stadig er væsentlige uafklarede juridiske spørgsmål og udfordringer, som først forventes afklaret i de kommende år.

I vores rolle som Databeskyttelsesrådgiver i KK, vil vi derfor i nogle tilfælde skulle anbefale at udsætte eller ændre projekter, hvis de regulatoriske krav ikke kan opfyldes under de givne omstændigheder eller i det tænkte set-up.

Vi vil primo 2025 opdatere vores notat til forvaltningerne om brug af personoplysninger i KI-løsninger, med særligt fokus på:

- Formål
- Hjemmel
- Leverandørforhold
- Tekniske og organisatoriske foranstaltninger

Formål

Når forvaltningerne ønsker at anvende KI til behandling af personoplysninger, skal der kunne formuleres et klart og tydeligt formål – hvilken behandling af personoplysninger, ønskes foretaget af den kunstige intelligens og hvorfor.

Det er vigtigt at formålet formuleres så konkret som muligt, så der ikke er tvivl om, hvad kommunen forventer af udbytte fra KI-modellen. Formålet bør være knyttet til en eller flere konkrete use-cases, der hver især skal vurderes på deres lovlighed.

En af de største udfordringer i KI-projekter er, at formål ved KI-projekternes opstart er for brede og ukonkrete.

Hjemmel

Det er en grundlæggende forudsætning for, at en forvaltning lovligt kan behandle personoplysninger ved brug af en KI-løsning, at der er identificeret det nødvendige hjemmelsgrundlag.

Udfordringen med at identificere den konkrete hjemmel er generelt, at lovgivningen på fagområderne ikke rummer brug af ny teknologi.

Det er vores klare forventning, at Datatilsynet i den kommende tid, vil komme med flere fortolkningsbidrag, i form af udtalelser og afgørelser, som kan afklare hvilke tilfælde, en offentlig myndighed kan gøre brug af KI i forbindelse med udøvelsen af den offentlige myndighedsopgave ligesom der må forventes ny lovgivning på fagområderne, der sætter rammerne, for brug af ny teknologi.

Et andet grundlæggende krav til lovlig behandling er, at behandlingen skal være gennemsigtig for de registrerede. Det betyder, at borgere skal kunne gennemskue hvad kommunens behandling af deres personoplysninger indebærer.

Dette kan i mange tilfælde være en udfordring, ved anvendelse af KI-løsning, da det ikke i alle tilfælde, er muligt at få et dybt nok indblik i, hvordan løsningen fungerer.

Leverandørforhold

Hvis kommunen anvender en leverandør til at udvikle en KI-løsning, der involverer behandling af personoplysninger, er det vigtigt at man har forholdt sig til dataansvaret og den instruks kommunen giver leverandøren, hvis der er tale om en databehandlerkonstruktion.

Leverandøren må ikke træne modellerne på KK-borgeres data, hvis leverandøren efterfølgende anvender den samme model, i de løsninger, der sælges til andre kunder.

Udfordringen består i, at kommunen ikke lovligt kan videregive oplysninger, som leverandøren anvender til egne formål, hvilket typisk er tilfældet, hvis leverandøren udvikler en KI-løsning til kommercielt formål. Derfor skal modellen og rigtige data holdes adskilt, indtil modellen er trænet færdig af leverandøren. Udvikling skal foretages med syntetiske data (test-data). Det gør sig også gældende i den løbende udvikling og eventuel træning af KI-modellen.

Tekniske og organisatoriske foranstaltninger

Endeligt er det vigtigt at sikre, at der bliver truffet tilstrækkelige tekniske og organisatoriske foranstaltninger. Det indebærer, at der bliver opsat klare regler for, hvad modellen må og ikke må, og at disse regler testes meget grundigt og vedvarende.

Det vil ikke være tilstrækkeligt udelukkende at basere sig på leverandørens forudgående test. Der skal ligeledes etableres løbende overvågning af, at modellen overholder de regler der er opstillet, f.eks. gennem logning af spørgsmål og svar.

Som en del af testen, vil det særligt være vigtigt at have fokus på risikoen for BIAS og hallucinationer.

BIAS betyder, at en sprogmodel kan have en forudindtaget viden om det den bliver spurgt om, på baggrund af de data, den er blevet trænet på. Det kan medføre skævheder og fordomme i de svar der bliver givet af modellen, og generelt resultere i faktuelt forkerte svar

Hallucinationer kan forekomme fordi sprogmodellerne grundlæggende set fungerer på den måde, at svarene er baseret på en statistisk udregning af, hvilket svar der er det mest korrekte. Det kan resultere i, at modellen baserer sit svar, på et forkert grundlag og dermed giver et opdigtet eller unøjagtigt svar.

Det er derfor vigtigt, at grundlaget for modellens træning vurderes, i forhold til om det træningsdatasæt den er trænet på, objektivt set er korrekt og at der ikke indgår en overvægt af særlige typer af data, frem for andre.

Organisatorisk skal kommunen sikre, at der eksisterer tilstrækkelige regler for medarbejderes brug af KI-løsninger. Medarbejdere skal instrueres og trænes i, hvad løsningen må anvendes til. Der skal ligeledes være regler for løbende overvågning af, hvordan medarbejderne anvender løsningen, for at sikre, at medarbejdere ikke bevidst eller ubevidst anvender løsningen til behandlinger der går imod instruksen.

4. Implementering af grundlæggende GDPR-krav

Modenheden i forvaltningernes arbejde med databeskyttelse er steget markant, og i løbet af det seneste år er fremdriften i arbejdet med, at sikre efterlevelse af de grundlæggende GDPR-krav, også blevet mærkbart forbedret.

De fleste forvaltninger er, eller tæt på at være, i mål med implementeringen af flere af de grundlæggende GDPR-områder. Dog er fremdriften stadig udfordret vedrørende udarbejdelse af risikovurderinger og konsekvensanalyser.

Risikovurderinger og konsekvensanalyser

Som anbefalet i statusrapporten for 2023 er der i KK i 2014 blevet justeret på konceptet for risikovurderinger af behandlingsaktiviteter jf. GDPR's artikel 32 og et koncept for hvis der, i tilfælde af høj risiko skal udarbejdes en konsekvensanalyse.

Risikovurderingskonceptet til behandlingsaktiviteter i KK er rettet mod GDPR-risici og indeholder ikke en vurdering af it-systemers risici. En risikovurdering for it-systemer hjælper med at identificere sårbarheder og trusler, der kan påvirke databeskyttelsen.

I en artikel 32-risikovurdering i henhold til GDPR er vurderingen af it-systemers risici en vigtig del. Artikel 32 fokuserer på kravet om passende tekniske og organisatoriske foranstaltninger, for at sikre et niveau af sikkerhed, der passer til risiciene for de registreredes rettigheder og frihedsrettigheder.

En fyldestgørende artikel 32-risikovurdering er udslagsgivende for, om der måtte være en høj risiko for den registrerede, og dermed krav om udarbejdelse af konsekvensanalyse.

For at sikre, at forvaltningerne kan udarbejde en fyldestgørende en artikel 32-risikovurdering og evt. i forhold til efterlevelsen af art. 35 at udarbejde en konsekvensanalyse, vil vi i samarbejde med Sikkerhedskontorerne i Koncern IT hurtigst muligt rådgive forvaltningerne om, hvilke sårbarheder og trusler der er relevante i forhold til vurdering af it-systemers risici der kan påvirke den registreredes rettigheder og hvor forvaltningerne kan søge oplysninger om etablerede tekniske og organisatoriske foranstaltninger, i forbindelse hermed.

5. Rådgivning, tilsyn og overvågning

Vi modtager løbende anmodning om rådgivning fra alle forvaltninger, og oplever en god dialog om databeskyttelsesretslige forhold og at forvaltningernes GDPR-funktioner er gode til at inddrage os tidligt.

Nedenfor gives en gennemgang af de opgaver der har fyldt mest i 2024.

Grundlæggende GDPR-krav

I de senere år har Københavns kommune arbejdet for at sikre en fælles tilgang til, at opfylde de grundlæggende GDPR-krav. Vi har gennem tilsyn, rådgivning og dialog med forvaltningernes GDPR-funktioner fulgt forvaltningernes indsatser i de senere år.

Der henvises til de forvaltningsspecifikke statusrapporter for yderligere information om status på de grundlæggende GDPR-krav og andre relevante forhold i forvaltningerne.

Overførsel af personoplysninger til tredjelande

Vi har fået flere spørgsmål om overførsel af personoplysninger til tredjelande, særligt USA. I statusrapporten for 2023 gav vi en status på Schrems-problematikken og det vedtagne overførselsgrundlag, Data privacy framework (DPF), som isoleret set løste problematikken med ulovlige overførsler til USA. Dette gælder stadig, hvis oplysninger bliver overført til amerikanske databehandlere, der er certificeret under frameworket og hvor personoplysninger befinder sig i USA.

Der er dog stadig en uløst problematik, i de tilfælde hvor der anvendes amerikanske underleverandører beliggende i EU. Dette er grundet i den amerikanske CLOUD ACT, der giver amerikanske myndigheder mulighed for at indsamle oplysninger om EU-borgere. Dette findes der ikke et lovligt overførselsgrundlag til, da amerikanske myndigheder ikke kan certificeres under DPF.

Det er et område med stor opmærksomhed, og Det europæiske databeskyttelsesråd (EDPB) kom for nyligt med en udtalelse omkring ansvar og forpligtelser i forhold til anvendelse og kendskab til underdatabehandlere og en skærpelse af reglerne til tredjelandsoverførsler. Denne udtalelse kom på baggrund af Datatilsynets henvendelse til EDPB vedrørende de udeståender der var i Chromebook-afgørelsen. Udtalelsen går imod Datatilsynet tidligere holdning om tilsigtet og utilsigtet overførsel. Som følge af dette, vil Datatilsynet komme med den sidste del-afgørelse i Chromebook-sagen samt opdatere deres cloud-vejledning, snarest muligt.

Vi anbefaler derfor, at forvaltningerne afventer Datatilsynets afgørelse og vejledning. Indtil vi modtager nyt fra Datatilsynet anbefaler vi, at der i forbindelse med eventuel indgåelse af nye aftaler, er særligt fokus på at gennemgå hele leverandørkæden og sikre, at usikre tredjelande som Kina og Indien, ikke er en del leverandørkæden.

Dataansvar

I år har vi fået flere spørgsmål om afklaring af dataansvar, herunder i hvilke tilfælde der skal indgås aftaler om fælles dataansvar eller om der er tale om en databehandlerkonstruktion.

Vi oplever, at der i flere tilfælde er indgået databehandleraftaler i leverandørforhold, hvor vi faktisk vurderer, at der slet ikke er tale om en databehandlerkonstruktion. Kommunen pålægges i den forbindelse forpligtelser som er unødvendige fx at føre tilsyn med sin databehandler.

På denne baggrund har vi valgt at sætte fokus på dataansvar som en indsatsområde i 2025, og vil i den forbindelse udarbejde rådgivningsmateriale som forvaltningerne kan bruge, når der skal vurderes dataansvar i fremtiden.

Borgerhenvendelser

I 2024 har vi oplevet en stigning i henvendelser fra borgere, der efterspørger konkret rådgivning om deres rettigheder efter databeskyttelsesreglerne.

Henvendelserne omhandler oftest retten til indsigt, retten til sletning eller spørgsmål på baggrund af et persondatabrud.

Generelt oplever vi en god dialog med de borgere, som ønsker viden om deres rettigheder efter GDPR, og derudover er det vores vurdering, at forvaltningerne samlet set, er gode til at håndtere de borgerhenvendelser, som videreformidles til deres behandling.

Servicebesøg

Servicebesøg er rettet mod decentrale enheder og skal ses som en udvidet rådgivningsindsats til de lokale ledelser på skoler, daginstitutioner, centre som ellers kun uddannes gennem de obligatoriske e-learningskurser.

Ved besøgene yder vi rådgivning om databeskyttelse til den lokale ledelse og medarbejdere, med afsæt i deres kerneopgaver.

Oftest får vi spørgsmål om, hvordan personoplysninger må behandles i en given situation og hvilken grad af behandlingssikkerhed der kræves.

Vi oplever stor interesse for vores servicebesøg og tilbagemeldingerne er positive. Servicebesøgene bliver fulgt op af vidensdeling med forvaltningerne omkring vores oplevelser og erfaringer fra besøgene.

I 2024 har vi gennemført 15 servicebesøg på tværs af BIF, BUF, SUF, KFF og SOF.
For 2025 påtænker vi at skabe yderligere værdi omkring servicebesøgene ved at tilbyde forvaltningerne konkret opfølgende sparring og rådgivningsbistand.

Sletning i eDoc

eDoc er kommunens ESDH-system, hvor der foretages størstedelen af den lovpligtige journalisering og er omfattet af arkivlovens krav om arkivering som følge af eDocs bevaringsværdighed.

Formålet med tilsynet var at påse reglerne for sletning, bevaringsværdighed og arkivering, i forhold til sager i eDoc, og hvordan reglerne håndteres i praksis.

Arkiveringen forestås af Stadsarkivet, som løbende har håndteret opgaven vedrørende arkivering efter reglerne.

Økonomiforvaltningen har siden 2023, har været i gang med et tværkommunalt sletteprojekt for at imødekomme udfordringerne med sletning i eDoc.

Vi har vurderet formål og scope af projektet, og er enige i de initiativer der er blevet igangsat og som ifølge det oplyste, forventes blive afsluttet primo 2025.

Vi vil i 2025 følge op på, at dokumenter i eDoc arkiveres og slettes i overensstemmelse med gældende regler.

Offentliggørelse af billeder på sociale medier

En afgørelse fra Datatilsynets vedrørende anvendelse af samtykke ved offentliggørelse at billeder af patienter på sociale medier, har givet anledning til drøftelser i KK. Datatilsynet udtalte alvorlig kritik og gav påbud om at slette opslag som indeholder helbredsoplysninger om patienter, som var offentliggjort på baggrund af samtykke.

Efter drøftelser med forvaltningernes GDPR-funktioner, har vi udarbejdet vi et notat til forvaltningerne om rammerne for offentliggørelse af billeder eller videoer på sociale medier af borgere og/eller medarbejdere i KK.

Formålet med notatet er at afdække, hvilke behandlingsgrundlag forvaltningerne bør overveje, når de ønsker at offentliggøre billeder/videoer med borgere og/eller medarbejder på sociale medier.

Håndtering af persondatabrud

Reglerne for vurdering og håndtering af persondatabrud fremgår af databeskyttelsesforordningens art. 33 og 34.

Her fremgår det, at persondatabrud skal anmeldes til Datatilsynet, medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Derudover skal den registrerede underrettes om bruddet, hvis der er en høj risiko.

Kommunen har generelt en god governance når det gælder håndteringen af persondatabrud.

For at ensrette og forbedre processen har vi udarbejdet en skabelon til vurdering af risici for de registrerede, i forbindelse med et persondatabrud, som alle forvaltninger har taget positivt imod.

Anvendelse af skabelonen vil kunne medvirke til, at forvaltningerne træffer de rigtige beslutninger i forhold til anmeldelser til Datatilsynet og eventuel underretning af de registrerede.

Vi vil i 2025 gennemføre yderligere rådgivningsaktiviteter herunder vurdere forvaltningernes anvendelse af risikovurderingsskabelonen.

6. Henvendelser fra Datatilsynet

Datatilsynet har i løbet af året afsluttet to tilsyn med KK, hvoraf det ene tilsyn gav anledning til kritik. Derudover har Datatilsynet udtalt alvorlig kritik i forbindelse med tilsynets opfølgning på et persondatabrud.

Fileshare – afsluttet tilsyn

Københavns Kommune har 7. maj 2024 modtaget en afgørelse fra Datatilsynet, hvor tilsynet udtaler alvorlig kritik i forbindelse med et anmeldt brud på persondatasikkerheden dateret 17. juni 2021.

Ved databruddet er det konstateret, at alle KK-medarbejdere med IT-adgang har haft adgang til et normalt lukket fildrev (Fileshare), med 3,7 mio. registreredes personoplysninger. I afgørelsen omtales desuden flere anmeldte brud på persondatasikkerheden relateret til brugen af Fileshare i Kommunen, hvor medarbejdere uden et arbejdsbetinget behov har haft adgang til personoplysninger.

I forbindelse med anmeldelsen har Datatilsynet anmodet kommunen om yderligere oplysninger. Koncern IT (KIT) har i den forbindelse beskrevet etablerede foranstaltninger før hændelsen og foranstaltninger der gennemføres efter hændelsen.

På baggrund af afgørelsen, har vi igangsat et ad hoc tilsyn, med det formål at sikre, at kommunen efter persondatabruddet har etableret passende tekniske og organisatoriske sikkerhedsforanstaltninger, i overensstemmelse med det til Datatilsynet oplyste.

Tilsyn med AULA – Afsluttet tilsyn

Tilsynet omhandlede KK`s efterlevelse af databeskyttelsesforordningen med særligt 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 blev udvidet til også at indeholde elementer af kommunens journalisering af børnesager, som Datatilsynet blev opmærksom på i forbindelse med en presseomtale i 2022.

Datatilsynets fandt på baggrund af KK´s besvarelser grundlag for at udtale kritik af kommunens konsekvensanalyse, idet den ikke indeholdte mindstekravene til en sådan analyse.

Herudover fandt Datatilsynet, at kommunen ikke til fulde havde godtgjort, at passende foranstaltninger var implementeret for at nedbringe alle de risici, kommunen havde identificeret. Hertil anbefalede Datatilsynet, at kommunen, i deres reviderede risikovurderingskoncept, strukturerer oplysningerne, så det bliver muligt at sammenligne risikovurderingerne før og efter implementeringen af foranstaltningerne, og at sammenhængen mellem foranstaltningerne og de enkelte risici fremgår tydeligt.

Tilsyn med behandlingssikkerhed – Afsluttet tilsyn

For at belyse og understøtte arbejdet med databeskyttelse i kommunerne har Datatilsynet siden 2021 ført tilsyn med kommuners modenhed i forhold til grundlæggende behandlingssikkerhed.

Tilsynet blev gennemført som et skriftligt tilsyn og indeholdt en spørgeramme på 77 spørgsmål fordelt på 15 forskellige emner indenfor behandlingssikkerhedsområdet.

Datatilsynet afsluttede tilsynet med bemærkning om, at de ikke havde udvalgt konkrete anbefalinger til KK, da kommunens besvarelse ikke gav anledning hertil. I stedet henviste Datatilsynet KK til at orienterer sig i de anbefalinger som de øvrige kommuner modtog.

Offentlige tilgængelige webarkiver– Igangværende tilsyn

Som et af Datatilsynets fokusområder for 2024 har Datatilsynet indledt et tilsyn med KK vedrørende implementering af den nye praksis for kommuners offentliggørelse af personoplysninger i offentlig tilgængelige webarkiver.

Formålet med tilsynet er at følge op på kommunernes inddragelse af tilsynets praksis, tilsynet har hertil angivet at KK derfor nødvendigvis ikke kan forvente en individuel tilbagemelding.
Kommunen har fremsendt besvarelse til tilsynet september 2024.

Databeskyttelsesrådgiverens udpegelse og rolle – Igangværende tilsyn

I marts 2023 indledte Datatilsynet, som en del af en koordineret undersøgelse i Det Europæiske Databeskyttelsesråd, en spørgeskemaundersøgelse særligt til Databeskyttelsesrådgiveren i alle landets kommuner.

Formålet med undersøgelsen var at skabe overblik over databeskyttelsesrådgiverens arbejde og eventuelle udfordringer forbundet hermed. Tilsynet oplyste, at resultatet af rapporten vil blive samlet i en national rapport, hvor tilsynet vil evaluere behovet for mere vejledning. Ligeledes vil undersøgelsen blive delt med tilsynsmyndigheder i andre lande i form af en samlet EDPB-rapport.

Kommunen afventer Datatilsynets nationale rapport.

Undersøgelse om skolebørns brug af Microsoft Teams – Igangværende tilsyn

På baggrund af en klagehenvendelse fra en borger i oktober 2023 vedrørende KK´s registrering af skolebørn i Microsoft Teams, har Datatilsynet indledt en nærmere undersøgelse heraf.

Borgerens klage blev også omtalt i vores statusrapport fra sidste år, og omhandler en episode, hvor et skolebarn modtog dødstrusler fra et andet barn fra en anden skole i kommunen. I den forbindelse har Datatilsynet bedt KK om at redegøre for de personoplysninger, der registreres på skolebørn i Microsoft Teams, hvilke formål og hjemmel, der ligger til grund for behandlingen, samt hvad de forskellige brugere i Microsoft Teams kan se af oplysninger om andre brugere. Herudover er kommunen også blevet bedt om at fremsende en risikovurdering.

Kommunen har besvaret Datatilsynet, og afventer tilbagemelding fra Datatilsynet.

7. DPO for selvejende institutioner med driftsoverenskomst

KK tilbyder vederlagsfrit en DPO-ordning til alle selvejende institutioner som har driftsoverenskomst med KK. Pr. 1. december 2024 er 146 selvejende institutioner omfattet af ordningen. Disse er fordelt på 110 daginstitutioner, 12 sociale institutioner og 24 plejehjem.

I 2024 har tilsyn været den overvejende aktivitet, hvor vi har ført tilsyn på over halvdelen af institutionerne. Ved de fysiske tilsyn har vi undersøgt det samlede databeskyttelsesniveau i institutionen. Ved de skriftlige tilsyn har vi undersøgt, om ledelsen løbende sikrer at de på institutionen besluttede regler og retningslinjer i forhold til databeskyttelse, efterleves i praksis. Alle tilsyn er afsluttet og rapporteret til ledelse og bestyrelse.

Resultatet af vores tilsyn viser, at institutionernes modenhed er øget, og databeskyttelse er blevet en mere naturlig del af hverdagen. For en del institutioner viste tilsynene behov for forbedringer hvilket har medført supplerende rådgivning eller opfølgningstilsyn, for at sikre et tilstrækkeligt databeskyttelsesniveau.

Vores væsentligste aktiviteter i 2024 er:

- 17 fysiske tilsyn
- 61 skriftlige tilsyn
- 86 rådgivningsopgaver
- 14 rådgivningsaktiviteter i forbindelse med lederskift
- 6 databrud, hvor der er søgt rådgivning i forbindelse med håndtering og anmeldelse til Datatilsynet
- 9 nyheder med anbefalinger og nye værktøjer
- 3 undervisningswebinarer – denne gang rettet mod institutionernes medarbejdere.
- On-boarding af 2 nye institutioner.

Der er planlagt tilsyn på de resterende institutioner i 2025.

København, den xx. januar 2025

Københavns Kommune Databeskyttelsesrådgiverfunktion

Jesper Andersen

Databeskyttelsesrådgiver for Københavns Kommune

Line Nymann Schoop Christian Cramer Kjelmann Lone Forsberg

Jonathan Rosenkrantz Brix Luna Stenberg Lind Anders Ettrup Gutfelt

Bilag 1 - 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. Hvis 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