DEN UAFHÆNGIGE KONTROL- OG RÅDGIVNINGSFUNKTION

STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

København Kommune

For året 2025

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 (herefter 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 Kontrol- og Rådgivningsudvalget og til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

2. Databeskyttelsesrådgiverfunktionen i Københavns Kommune

Borgerrepræsentationen har besluttet, at Lederen af Den Uafhængige Kontrol- og Rådgivningsfunktion er kommunens Databeskyttelsesrådgiver, jf. § 27, stk. 10, i Styrelsesvedtægten for KK.

Databeskyttelsesrådgiverens opgaver er fastlagt i lovgivningen om databeskyttelse samt i KK's Informationssikkerhedsregulativ.

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

Samspil mellem informationssikkerhed, databeskyttelse og anden lovgivning

KK har igangsat et arbejde med at etablere et samlet ISMS (information security management system), som skal fastlægge de overordnede strategiske rammer, herunder mål, roller og krav til styring af informationssikkerhed på tværs af hele kommunen. Det er meget positivt at KK arbejder for at skabe en systematisk tilgang til styringen af informationssikkerheden, som i sidste ende kan bidrage til en bedre databeskyttelse for borgere og medarbejdere.

Et ISMS indeholder alle de politikker, procedurer, retningslinjer som en organisation skal følge, og sikrer at alle lovkrav håndteres uanset om der er tale om GDPR, NIS2 eller AI-forordningen.

Det er vores anbefaling, at KK har fokus på at skabe ét overordnet rammeværk, hvor alle lovkrav der påvirker styringen af informationssikkerheden, bliver tilkoblet. KK vil dermed få ét sted hvor al styring begynder og slutter.

Alvorlig sag om misbrug af adgang til CPR-registeret

I sommeren 2025 blev en meget alvorlig sag om misbrug af adgang afdækket. En studentermedhjælper som var ansat i Kultur- og fritidsforvaltningen i KK, blev anholdt og sigtet for at have misbrugt sin adgang til CPR-registeret til brug for planlægning af drab med tilknytning til bandemiljøet.

Der var tale om en lang række borgeres CPR-numre som studentermedhjælperen uretmæssigt brugte til at fremsøge yderligere personoplysninger om borgere, og i nogle tilfælde med henblik på at anvende oplysningerne til kriminelle formål.

I de senere år og før denne sag indtrådte, har vi haft meget fokus på at rådgive KK om hvordan man bedst forebygger, opdager og håndterer sager om uberettigede opslag. Det er vores anbefaling, at der skal etableres gode processer for adgangsstyring og logkontrol og der skal være klare retningslinjer for, hvilke sanktioner en medarbejder skal mødes med, hvis vedkommende slår borgere eller medarbejdere op, uden at der er et arbejdsbetinget behov.

Vi fik tidligt i 2025 i samarbejde med Koncernservice udarbejdet et notat om håndtering af uberettigede opslag på tværs af KK.

Uddannelse af medarbejdere

Vi ser et stigende fokus på uddannelse af medarbejdere og ledelse i de reguleringer der kommer fra EU. NIS2 er et godt eksempel på regulering, som stiller krav om uddannelse af ledelsen i grundlæggende cybersikkerhed.

Vi bemærker at KK har besluttet at nedsætte frekvensen for den obligatoriske e-learnings uddannelse af medarbejdere og ledelse i Informationssikkerhed og databeskyttelse fra hvert 2. år til nu kun hvert 4 år.

Vi anbefaler, at niveauet for uddannelse af medarbejdere og ledelse revurderes og fastsættes ifm. KK's ISMS-projekt.

Kunstig intelligens og ny lovgivning på vej?

Anvendelse af kunstig intelligens (herefter AI) er noget, som KK kommer til at arbejde videre med i fremtiden, og det er derfor væsentligt at sikre, at der er fokus på hvilke regler der gælder når man anvender AI til behandling af personoplysninger.

Vi oplever at KK arbejder fornuftigt med de regulatoriske krav, der gælder når man vil bruge personoplysninger i forbindelse med en AI-løsning, men forvaltningerne er samtidig underlagt et stort pres fra leverandører. Vi oplever i stigende grad, at KK's leverandører indbygger AI-løsninger ind i eksisterende fagsystemer, hvilket kan være en udfordring hvis det er KK's vurdering, at der ikke er hjemmel til at ibrugtage AI-løsningen. Den største udfordring lige nu er, at den sektorlovgivning som forvaltningerne opererer under, ikke er klar til brug af AI, når der er tale om indgribende behandling overfor borgere eller medarbejdere. Vi ved at flere forvaltninger er gået i dialog med ressortministerierne om behovet for t lovgivning, der giver hjemmel til at bruge AI såsom beslutningsstøtte overfor borgere. Vi følger nøje med i udviklingen.

Rådgivning og tilsyn

I 2025 har vi haft øget fokus på rådgivning af forvaltningernes GDPR-funktioner. Emnerne har været mange, men særligt har fokus været på AI, persondatabrud og arbejdet med risikovurderinger og konsekvensanalyser. Vi har i første halvår haft en massiv indsats på håndtering af persondatabrud, hvor alle forvaltninger har deltaget aktivt i dialogen. I andet halvår udførte vi et tilsyn for at følge op på, om vores indsatser havde haft en effekt. Tilsynet viste, at der generelt er fremgang på området.

Antallet af borgerhenvendelser er fortsat stigende, og vi vejleder og rådgiver dagligt borgere om deres rettigheder.

Igen i år har vi haft fokus på servicebesøg, hvor vi understøtter GDPR-funktionerne ved at yde konkret rådgivning og vejledning til decentrale enheder i KK. For første gang har vi besøgt alle forvaltninger, hvilket er meget positivt og vi oplever positiv feedback og efterspørgsel på at udbrede konceptet til flere fagområder, indenfor hver forvaltning.

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

Fokusområder i 2026

Vi vil fortsat have fokus på at understøtte GDPR-funktionerne med rådgivning fremfor tilsyn, da det skaber størst værdi for kommunen. I 2026 vil vi fortsætte det gode samarbejde med forvaltningerne i KK og have særligt fokus på brug af AI, herunder AI-governance, uddannelse af medarbejdere og persondatabrud.

God læselyst!

4. Ét fælles rammeværk i KK

Når man ønsker at skabe en samlet governance-struktur handler det om at skabe et fælles sprog og en fælles tilgang til de lovkrav, som organisationen skal styre efter. Mange organisationer har regler, procedurer og retningslinjer, som er blevet opdateret over tid, skrevet af forskellige personer i organisationen og som afspejler det fokus, som måtte have været fremherskende på tidspunktet for udarbejdelsen. Resultatet er en fragmenteret styring, hvor krav fra fx GDPR, NIS2, AI-forordningen mv. fører til mange og ofte overlappende regler, som håndteres og fortolkes forskelligt på tværs af organisationen.

Det er vores vurdering, at KK på GDPR-området har en struktureret tilgang til regler og retningslinjer, men at der mangler sammenhæng til andre lovkrav såsom AI-forordningen og NIS2, som har mange overlap og krav der mest effektivt håndteres samlet.

Derfor er det vores anbefaling, at KK har fokus på at skabe ét overordnet rammeværk, hvori alle informationssikkerhedsmæssige krav, der stammer fra lovgivning, bliver håndteret.

Etablering af et ISMS i Københavns kommune

KK følger ISO27001-standarden som er et internationalt anerkendt rammeværk for styring af informationssikkerheden. KK har i 2025 igangsat et større arbejde med at få etableret et ISMS på tværs af alle forvaltninger, hvilket er positivt. Hvis man som organisation har en god informationssikkerhed, hvor styringen kommer fra ledelsen, giver det et godt grundlag for beskyttelse af borgere og medarbejderes data.

Et ISMS er en ledelsesmodel og et rammeværk, der hjælper en organisation med at styre og beskytte sine informationer ved at fastsætte regler, processer og kontroller for sikkerhed. Et ISMS hjælper med at beskytte borgernes data, sikre stabile og robuste IT-løsninger samt skabe klare processer for, hvordan man identificerer og håndterer risici for både kommunen og borgerne. Lidt forsimplet giver et ISMS en god styring og færre sårbarheder.

Det er vores vurdering, at korrekt og tilstrækkelig implementering af et ISMS i KK, vil kunne skabe den gode samlede governance-struktur, som der er behov for.

En samlet tilgang til risikovurderinger

Vi vurderer at ISMS-arbejdet er et vigtigt led i KK´s mulighed for at kunne dokumentere, hvordan man arbejder med informationssikkerheds-risici i kommunen, ligesom arbejdet vil have positiv betydning for beskyttelsen af borgernes personoplysninger.

ISMS'et kræver, at man arbejder systematisk med risici, så man kan finde ud af, hvad der kan gå galt, vurdere hvor alvorligt det er, og beslutte at håndtere det ved at vælge passende sikkerhedstiltag og derefter løbende holde øje med, om noget har ændret sig.

Vi har i de tidligere års statusrapporter påpeget, at fremdriften i arbejdet med udarbejdelse af risikovurderinger af behandlingsaktiviteter og konsekvensanalyser er

udfordret. Dette på trods af, at vi grundlæggende vurderer, at forvaltningernes modenhed i arbejdet med grundlæggende GDPR-krav er steget markant. Udfordringen består i, at KK's nuværende koncepter for risikovurderinger af behandlingsaktiviteter og IT-systemer ikke hænger sammen. Der arbejdes fragmenteret med risikovurderinger på tværs af IT og de organisatoriske rammer. GDPR stiller krav om, at man både forholder sig til risici ved den menneskelige håndtering af personoplysninger, men også risici i IT-systemer, som kan påvirke den registreredes rettigheder.

Vi vurderer, at etableringen af et ISMS vil kunne skabe rammerne for KK's tilgang til arbejdet med risici og kan skabe den sammenhæng og systematik, som der er behov for. Vi vil løbende overvåge, om risikovurderingsarbejdet får skabt den sammenhæng, som vi har efterspurgt, så forvaltningerne er i stand til at udarbejde fyldestgørende risikovurderinger efter artikel 32 i GDPR.

5. Status på arbejdet med kunstig intelligens

2025 har været præget af AI på mange måder. Vi har rådgivet alle forvaltningerne om mulighederne for at anvende AI til at understøtte forvaltningernes opgaver. Størst har fokus været på mulighederne for at anvende AI til borgerrettede løsninger og løsninger, som understøtter forvaltningernes sagsbehandlere på de mere borgernære områder.

Vi har i februar 2025 opdateret vores notat om AI, hvor vi beskriver, hvilke juridiske vurderinger der bør foretages, inden man påbegynder behandling af personoplysninger i en AI-løsning. Det har særligt været opdateringer vedrørende lovhjemmel og udviklingssamarbejder med leverandører.

Datatilsynet er kommet med en række afgørelser og udtalelser om brug af AI, ligesom Datatilsynet har afsluttet den regulatoriske sandkasse, som Sundhed- og omsorgsforvaltningens TALT-projekt, var en del af.

Herudover har EU-domstolen afsagt en dom vedrørende brugen af pseudonymiserede personoplysninger. Dommen handler om, hvorvidt pseudonymiserede oplysninger altid skal anses for at være personoplysninger, hvordan det skal vurderes, om oplysningerne er personhenførbare og fra hvis perspektiv vurderingen af, om oplysningerne er personhenførbare, skal foretages.

Endelig er AI-forordningen ved at blive implementeret i Europa, og vi konstaterer, at der er en række overlap til GDPR-reglerne, hvilket taler for en samlet håndtering.

TALT-projektet

KK's Sundheds- og omsorgsforvaltning (SUF) deltog i 2024 i Datatilsynets regulatoriske sandkasse for AI-projekter. "TALT-projektet" havde til formål at understøtte udarbejdelse af journalnotater, b.la. fra tale til tekst.

Dialogen med Datatilsynet gik primært på lovhjemmel og en drøftelse med SUF omkring mulige hjemmelsgrundlag i den relevante faglovgivning, som SUF havde

identificeret. Datatilsynet vurderede, at lovhjemlerne ikke var tilstrækkeligt klare, henset til den indgribende behandling som AI-modellen foretog.

Resultatet af sandkasseprojektet blev derfor, at SUF, i samråd med Datatilsynet, kontaktede det relevante ressortministerium med henblik på at få indsat en bestemmelse i særlovgivningen, der kan understøtte den påtænkte behandling. Vi afventer udarbejdelsen af lovforslaget.

Vi oplever generelt stigende interesse for området, og at flere forvaltninger i KK arbejder for at få hjemmel til at gøre brug af AI-modeller til behandling af personoplysninger af indgribende karakter. Vi følger udviklingen tæt.

Hvornår kræver AI-løsningen klar lovhjemmel?

AI er blevet et populært hjælpeværktøj, uanset hvilken opgave man måtte stå overfor, og det er vores oplevelse, at der i kommunen også er en stigende interesse for at integrere og anvende AI, på forskellige fagområder for at opnå større effektivitet. Det kan dog være vanskeligt at vurdere, hvorvidt en behandling af borgeres eller medarbejderes oplysninger ved brug af AI, vil kræve en særlig klar hjemmel i lovgivningen, eller om den påtænkte behandling ved brug af AI kan rummes indenfor den allerede eksisterende lovgivning.

I Datatilsynets udtalelse af 5. november 2025 om hjemmel til drift af en AI-løsning på SU-området fremgår det, at kravene til klarheden af hjemmel vurderes ud fra, hvor indgribende behandlingen er overfor de registrerede, uanset om behandlingen måtte være bebyrdende eller begunstigende. I udtalelsen fremgår det endvidere, at det i vurderingen skal inddrages, hvilke oplysninger der behandles, samt hvilke personer der behandles oplysninger om. Det betyder, at det vil tale for, at behandlingen er af indgribende karakter overfor de registrerede hvis AI-løsningen vil behandle følsomme oplysninger om sårbare registrerede, herunder ældre, børn mm.

Det er dog ikke kun vurderingen af de registrerede og deres oplysninger, der ligger til grund for den endelige vurdering af, hvor indgribende behandlingen er. Det fremgår således af udtalelsen, at AI-løsningens output også har afgørende betydning for, hvor indgribende løsningen er at anse, herunder om løsningen genererer forudsigelser eller fungerer som beslutningsstøtte til afgørelser, som kan have konsekvens for de registreredes forhold. Herudover kan det udledes af tilsynets udtalelse samt deres vejledning om offentlige myndigheders brug af kunstig intelligens, at løsningen vil anses som værende indgribende jo større konsekvens løsningens output har på de registreredes forhold, eksempelvis hvis løsningen fungerer som beslutningsstøtte i forbindelse med en afgørelse, der vedrører den registreredes økonomiske, uddannelsesmæssige, sociale, sundhedsmæssige eller lignende forhold.

Endelig fremgår det af Datatilsynets udtalelse, at der i den samlede vurdering af hvor indgribende AI-løsningen er at anse overfor de registrerede, bør indgå, om den pågældende behandling af de registrerede personoplysninger er gennemsigtig, således at det er klart for de registrerede, at deres oplysninger vil være genstand for en behandling, hvor der anvendes AI.

Vi følger Datatilsynets praksis, når vi rådgiver KK om brugen af AI.

Særlig opmærksomhed på AI-udviklingssamarbejder

I vores dialog med forvaltningerne har vi haft fokus på leverandørforholdet, når KK ønsker at indgå et samarbejde med en leverandør, til udvikling af en AI-løsning. Vi oplever et stort pres fra leverandørerne i forhold til at få udviklet løsninger på KK-data.

Hvis kommunen anvender en leverandør til at udvikle en AI-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 løsninger, der sælges til andre kunder. Udfordringen består i, at kommunen ikke lovligt kan videregive oplysninger, som leverandøren anvender til egne formål, hvilket kan være tilfældet, i forbindelse med udvikling af en AI-løsning, med det formål at sælge løsningen til andre kunder. Derfor skal motoren og data holdes adskilt, indtil modellen er trænet færdigt af leverandøren. Udvikling skal foretages med syntetiske data (test-data) og ikke KK's data.

Pseudonymisering og AI

Vi har i november 2025 udarbejdet et rådgivningsnotat til forvaltningerne angående pseudonymisering. Notatet udspringer af afgørelsen kaldet "SRB-sagen" fra EU-domstolen, der angik spørgsmål om, hvorvidt pseudonymiserede oplysninger altid skal anses for at være personoplysninger, hvordan det skal vurderes, om oplysningerne er personhenførbare, og fra hvis perspektiv vurderingen af, om oplysningerne er personhenførbare, skal foretages.

Efter EU-domstolens afgørelse har der været en del debat om rækkevidden og fortolkningen af afgørelsen. Datatilsynet har derfor ad to omgange officielt givet deres fortolkning og præcisering af, hvad der gælder. Vi følger Datatilsynets tilkendegivelser.

EU-domstolen kom frem til, at pseudonymiserede oplysninger ikke altid skal anses for at være personoplysninger, hvilket stemmer overens med den hidtidige praksis. Vurderingen skal inddrage alle rimelige hjælpemidler og konteksten for behandlingen. Det blev dog konkret i afgørelsen slået fast, at når der er tale om en databehandlerkonstruktion, så vil det være den dataansvarliges behandling, der skal være udgangspunktet for vurderingen, når man i sidste ende skal vurdere, om den behandling, som databehandleren foretager på vegne af den dataansvarlige, er en behandling af personoplysninger.

Datatilsynet har præciseret betydningen af afgørelsen og understreger, at en databehandler kun kan behandle oplysninger efter instruks fra den dataansvarlige, og at databehandleren derfor ikke kan foretage en behandling på vegne af den dataansvarlige, som den dataansvarlige ikke selv har hjemmel til at foretage.

Man kan derfor ikke pseudonymisere personoplysninger og overlade dem til en databehandler, for at få databehandleren til at foretage en behandling, som man ikke selv som dataansvarlig har hjemmel til.

I en AI-kontekst er afgørelsen meget relevant. Som følge af afgørelsen, kan man som dataansvarlig ikke løse en hjemmelsproblematik med behandling af personoplysninger

ved hjælp af en AI-model ved at pseudonymisere personoplysningerne, inden de overlades til en, databehandler med henblik på, at databehandleren anvender en AI-model til at foretage en behandling som den dataansvarlige ikke har hjemmel til. I sådan et tilfælde, skal vurderingen af, om oplysningerne er personhenførbare, foretages ud fra den dataansvarliges perspektiv. Det vil medføre at de overladte oplysninger skal anses for personhenførbare for databehandleren, selvom denne reelt ikke kan udlede, hvem oplysningerne omhandler.

AI forordningen

Det er ikke kun GDPR-reglerne, der skal iagttages, når man ønsker at anvende AI. AI-forordningen gælder både for dem der udvikler, idriftsætter og anvender AI, og dele af forordningen er trådt i kraft i 2025. AI-forordningen har mange overlap til GDPR-reglerne, og vi følger naturligvis med i KK's håndtering af krav fra AI-forordningen i samspil med GDPR.

KK bør allerede nu være opmærksomme på de forbudte former for AI-praksis, som AI-forordningen opregner, og at det følger af forordningen, at der skal sikres et tilstrækkeligt niveau af AI-færdigheder hos alle de medarbejdere, som er involveret i driften eller anvendelsen af et AI-system. Det betyder at KK skal have fokus på medarbejdernes tekniske viden, erfaring og uddannelse, den kontekst, som AI-løsningen anvendes i, og de personer som AI-systemerne skal anvendes på.

6. Uddannelse af medarbejdere

Den teknologiske udvikling og den stigende cybertrussel fører til regulering, der bl.a. stiller øgede krav til uddannelse af medarbejdere og ledelse.

Medarbejderfejl anses af mange for den største trussel mod cybersikkerhed, og vi ser derfor mere regulering på netop dette område. NIS2 stiller også skærpede krav til ledelsens håndtering og styring af cybersikkerheden.

På trods af denne udvikling har vi i 2025 kunnet konstatere, at frekvensen for KK-medarbejderes uddannelse i GDPR og informationssikkerhed sat ned fra 2 år til 4 år. Økonomiudvalget besluttede tilbage i 2018, at det er obligatorisk for medarbejderne at gennemføre en uddannelsen hvert 2. år.

Dette giver anledning til bekymring og en konkret anbefaling om, at KK forholder sig til de stigende krav om øget awareness hos både medarbejdere og ledere.

Som led i KK's ISMS-projekt er der nedsat en arbejdsgruppe for awareness og uddannelse, og det anbefales at niveauet for uddannelsesindsatser løftes i den sammenhæng.

I 2026 vil vi have øget fokus på KK's tilgang til uddannelse af medarbejdere.

7. Uberettigede opslag

I år har vi været involveret i flere sager om medarbejdere, der uberettiget tilgår oplysninger, som de ikke har arbejdsbetinget behov for at tilgå.

På statsligt niveau offentliggjorde man i 2025 en undersøgelse om personer, der i offentlig tjeneste eller hverv, udøver eller muliggør udøvelse af negativ social kontrol over borgere i æresrelaterede konflikter. I rapporten er der eksempler på hvordan offentligt ansattes handlinger – bevidste eller ubevidste – kan medvirke til at opretholde eller forstærke udøvelsen af negativ social kontrol. Det er blandt andet sket ved, at medarbejdere har tilgået eller videregivet personoplysninger uberettiget, eller har presset borgere til ikke at flytte på krisecenter eller søge skilsmisse. Der er også eksempler på, at familiemedlemmer eller netværk med adgang til offentlige stillinger, der giver mulighed for at tilgå eller misbruge fortrolige oplysninger, kan være en barriere for borgerens mulighed for at søge hjælp.

Rapporten og konkrete sager i KK gav anledning øget dialog med Koncern IT omkring sikkerhedsforanstaltninger med fokus på både at opdage og forebygge uberettigede opslag, men også en dialog om den personalejuridiske håndtering, særligt i forhold til fastlæggelse af et ens sanktionsniveau på tværs af KK.

Vi fik i samarbejde med Koncernservice udarbejdet et notat om håndtering af uberettigede opslag, som fastlægger rammerne, herunder hvilke skærpende og formildende omstændigheder der kan indgå i den personalejuridiske vurdering. Dertil fastlægger notatet rammerne for, hvornår Koncernservice kan forelægge en konkret sag for Økonomiudvalget.

I juli 2025 blev den såkaldte "CPR-sag" omtalt i medierne. En ansat studentermedhjælper i Kultur- og fritidsforvaltningen blev sigtet for at have foretaget en række uberettigede opslag på borgeres CPR-numre. I nogle tilfælde er der ifølge politiet videregivet oplysninger til uvedkommende, der potentielt er anvendt til kriminelle formål.

KK håndterede sagen som en databrudssag og underrettede både Datatilsynet og de registrerede. Datatilsynet er efterfølgende gået ind i sagen, og vi afventer deres tilbagemelding. Der pågår ligeledes en strafferetlig efterforskning. Denne varetages af National Enhed for Særlig Kriminalitet (NSK).

8. Rådgivning, tilsyn og overvågning

Vores opgaver er i overvejende grad fastlagt i en aktivitetsplan, som er behandlet og godkendt i Revisionsudvalget. I 2025 har vi ændret vores tilgang, så vi i højere grad fokuserer på rådgivning, frem for at føre et højt antal af tilsyn. Vi ønsker at sikre, at forvaltningerne får målrettet rådgivning, som kan understøtte og opretholde en stærk GDPR-compliance.

Rådgivning til forvaltningerne

I 2025 har vi modtaget et stigende antal anmodninger om rådgivning fra forvaltningerne, og vi oplever en god dialog om databeskyttelsesretlige forhold, ligesom forvaltningernes GDPR-funktioner er gode til at inddrage os rettidigt.

Nedenfor gives en gennemgang af de opgaver der har fyldt mest i 2025.

Servicebesøg

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

Vi yder rådgivning om databeskyttelse til den lokale ledelse og medarbejdere, med afsæt i deres kerneopgaver, hvor vi kan medvirke til at skabe klarhed over databeskyttelsesretlige hensyn i arbejdsgange.

I 2025 har vi været på besøg i alle forvaltninger fordelt over 23 enheder. Inden servicebesøgene fik GDPR-funktionerne mulighed for at vidensdele databeskyttelsesretlige temaer og udfordringer, som GDPR-funktionen kendte til i deres forvaltning, så servicebesøgene kunne målrettes bedre.

Vi oplever stor interesse for vores servicebesøg, der får positive tilbagemeldinger, og oplever også, at enhederne får et større fokus på databeskyttelse efter vores servicebesøg.

I 2026 vil vi fokusere vores servicebesøg til enheder, der hovedsagelig har kontakt med borgere eller medarbejdere, og/eller har en stor variation i deres opgaver, da vores erfaring fra de foregående år har vist, at det er hos disse enheder, at vi skaber den bedste værdi for både enhederne og de borgere, de betjener.

Dialogmøder om AI

Muligheden for anvendelse af AI fylder mere og mere i forvaltningerne, og har indtil videre givet en række udfordringer i forhold til at forstå og håndtere regler og andre forudsætninger, der skal være opfyldt, hvis AI løsninger skal etableres.

Det har givet anledning til, at vi i 2025 har afholdt to dialogmøder med forvaltningerne om AI.

Dialogen tog afsæt i Datatilsynets anbefalinger og vores seneste rådgivningsnotat om AI. Formålet var blandt andet at finde en fælles referenceramme for, hvordan AI skal defineres, hvordan en given løsning kan vurderes i forhold til, om der er tale om AI, og de trin, der skal gennemføres, inden en AI løsning kan iværksættes.
Forvaltningerne har efterfølgende tilkendegivet, at dialogmøderne har bidraget til øget viden på området.

Persondatabrud

I 2023 påbegyndte vi en systematisk overvågning af forvaltningernes registrerede databrud. Overvågningen viste, at forvaltningernes håndtering af databrud ofte var behæftet med en usikkerhed og/eller varierende vurdering af risikoen for den registrerede.

Dette var baggrunden for at vi i 2024 og 2025 gennemførte en række rådgivningsaktiviteter, fælles dialogmøder og 1:1 møder med den enkelte forvaltning, hvor vi blandt andet præciserede reglerne men også drøftede forvaltningernes udfordringer. I samme forbindelse fremlagde vi et forslag til en skabelon til vurdering af risici for den registrerede, for at understøtte de nødvendige beslutninger og dokumentation. Endelig tog vi initiativ til et møde med Datatilsynet, hvor regler om anmeldelse blev præciseret.

Vi har nu gennemført det afsluttende tilsyn på området. Her kan vi konstatere, at der er sket mærkbare forbedringer, der betyder, at forvaltningerne i overvejende grad vurderer og dokumenterer databrud korrekt at brudene anmeldes til Datatilsynet, og at de registrerede underrettes som forordningens regler foreskriver.

Dataansvar

Som en del af vores årsplan 2025 har vi gennemført en større rådgivningsopgave, hvor vi undersøgte, hvordan man i praksis kan bestemme placering af ansvaret for data, når kommunen har et samarbejde med en ekstern part.

Opgaven udsprang af de mange henvendelser, som vi løbende havde modtaget, og som indikerede et behov for at undersøge området til bunds og bidrage med en mere tværgående rådgivning.

I samarbejde med alle forvaltninger og med god dialog med Koncern IT, udarbejdede vi "Gode råd til at bestemme dataansvarsplacering", som vi forventer kan medvirke til en bedre indsigt i et komplekst område.

9. Henvendelser fra Datatilsynet

Datatilsynet har i løbet af året afsluttet ét tilsyn, foretaget to høringer i konkrete sager og i ét tilfælde anmodet om oplysninger på baggrund af en meget omtalt sag i medierne.

Tilsyn med overvågning af ansatte – afsluttet

Som et af Datatilsynets fokusområder i 2025 indledte de et tilsyn i form af en kortlægning af omfanget og karakteren af den overvågning, der finder sted med henblik på kontrol af ansatte hos både private og offentlige arbejdsgivere.

Formålet med kortlægningen var at opnå kendskab til omfanget og karakteren af den overvågning, der finder sted, med henblik på kontrol af ansatte hos såvel private som offentlige arbejdsgivere.

Datatilsynet har afsluttet tilsynet og oplyser at KK's besvarelse vil indgå i planlægningen af Datatilsynets tilsyns- og vejledningsaktiviteter i de kommende år.

Datatilsynet bemærker afslutningsvis, at de ikke har undersøgt, om overvågningen af kommunens ansatte er sket i overensstemmelse med databeskyttelsesreglerne.

Høring om videregivelse af oplysninger til Indien – afsluttet

En landsdækkende politisk forening kontaktede Datatilsynet med en række opklarende spørgsmål, angående et af KK's systemer.

Spørgsmålene gik hovedsageligt på behandlingen af personoplysninger om foreningen og dennes bestyrelse, om der skete overførsel til et tredjeland (Indien) og om adgangen til data i pågældende tredjeland. Datatilsynet anmodede i den forbindelse svar på spørgsmålene fra den politiske forening.

Datatilsynet oplyste, at tilsynet ikke ville foretage sig yderligere efter besvarelsen fra KK, og sagen er dermed afsluttet.

Høring om log på personalesager på baggrund af klage – ikke afsluttet

På baggrund af en klagehenvendelse vedrørende afslag på indsigt i logoplysninger, stillede Datatilsynet KK opklarende spørgsmål.
Spørgsmålene omhandlede omfanget af logning, opbevaring af logfiler og andre foranstaltninger omkring tilgangen til personalefiler i KK's system.
KK har besvaret Datatilsynet, og afventer tilbagemelding fra Datatilsynet.

Anmodning om oplysninger ifm. Misbrug af CPR-adgang – ikke afsluttet

På baggrund af Kultur- og fritidsforvaltningens (KFF) anmeldelse af et persondatabrud og massiv medieomtale, anmodede Datatilsynet om yderligere oplysninger. Sagen omhandlede en medarbejder i som havde misbrugt sin adgang til Det Centrale Personregister (CPR) ved at have foretaget cirka 1.700 mistænkelige opslag på borgere, og at medarbejderen i visse tilfælde havde videregivet oplysninger om borgere til uvedkommende. KK har besvaret Datatilsynet, og afventer tilbagemelding.

10. DPO for selvejende institutioner med driftsoverenskomst

KK tilbyder vederlagsfrit en DPO-ordning til alle selvejende institutioner som har driftsoverenskomst med KK. Pr. 1. december 2025 er 143 selvejende institutioner omfattet af ordningen. Disse er fordelt på 108 daginstitutioner, 11 sociale institutioner og 24 plejehjem.

Året 2025 har været en forlængelse af det forrige års tilsynsaktivitet, hvor målet har været at engagere alle de selvejende institutioner med minimum ét tilsyn over en 2-årig periode. Ligesom sidste år har vi i år, ud fra en risikobaseret tilgang, gennemført både fysiske og skriftlige tilsyn.

Ved de fysiske tilsyn har vi undersøgt det samlede databeskyttelsesniveau i institutionen igennem en fast spørgerammer og stikprøver i institutions sletterutiner. Ved de skriftlige tilsyn har vi undersøgt, om ledelsen løbende sikrer, at institutionens regler og retningslinjer i forhold til databeskyttelse efterleves i praksis. Alle tilsyn er afsluttet og rapporteret til ledelse og bestyrelse.

Det overvejende billede, som tilsynene har efterladt både i 2024 og i år, har været en øget modenhed i forhold til at iagttage databeskyttelsesretlige pligter hos institutionerne, samt et ønske om og vilje til at udvise ansvarlighed i behandlingen og indarbejdelsen af databeskyttelse i deres daglige arbejde. Det kommer til udtryk ved, at vi ofte oplever opfølgende rådgivningsforespørgsler under og efter vores tilsyn, samt et større fokus på persondatabrud i perioden efter vores tilsyn. Generelt har tilsynsaktiviteterne vist sig effektive i at skabe fornyet fokus på databeskyttelse og beskyttelse af personoplysninger.

- Vores væsentligste aktiviteter i 2025 har været:
- 17 fysiske tilsyn
- 41 skriftlige tilsyn
- 61 selvstændige rådgivningsopgaver
- 11 databrud, hvor der er søgt rådgivning i forbindelse med håndtering og anmeldelse til Datatilsynet
- 8 nyheder med anbefalinger og nye værktøjer
- On-boarding af 2 nye institutioner

For alle de selvejende institutioner, der er med i ordningen, er der planlagt en ny 2-årig periode med et fokuseret tilsyn på viden og uddannelse hos medarbejderne i institutionerne, da medarbejderne er første forsvarslinje i arbejdet med databeskyttelse, og derfor er en vigtig del af institutionernes samlede indsats.

København, den 25. februar 2026

Københavns Kommune Databeskyttelsesrådgiverfunktion

Ingeborg Gade

Databeskyttelsesrådgiver for Københavns Kommune

Line Nymann Schoop Christian Cramer Kjelmann Anders Ettrup Gutfelt

Jonathan Rosenkrantz Brix Luna Stenberg Lind