INTERN REVISION

STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

Københavns Kommune

For perioden 1. oktober 2022 til 31. december 2023

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Indledning

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance, udarbejder Databeskyttelsesrådgiveren årligt en statusrapport.

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

Der er desuden udarbejdet en delrapport pr. forvaltning, som omhandler mere 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

Governance

I statusrapporten for 2022 fremhævede vi behovet for at etablere en governance i Københavns Kommune, som kunne skabe klarhed over, hvordan de databeskyttelsesretlige opgaver løses bedst muligt med fokus på at gøre tingene ensartet, højne niveauet samt løse opgaverne på en mere omkostningseffektiv måde.

I forlængelse heraf vedtog IT-kredsen i februar 2023 fire aktiviteter til at styrke organisering, roller og ansvar, og der blev etableret et program, som har til formål at styrke rammerne for at opnå en tilstrækkelig høj grad af regelefterlevelse på databeskyttelsesområdet. Primo 2024 har Programmet for Databeskyttelse udarbejdet fire leverancer som forventes implementeret i 2024.

Det er vores vurdering, at vores anbefaling fra 2022 vedrørende forbedret governance vil være opfyldt, hvis programmets leverancer implementeres som forventet.

Implementering af regler og retningslinjer på væsentlige områder

I forhold til implementering af regler og retningslinjer har der været fremgang i 2023, og forvaltningerne har arbejdet godt med fortegnelser, og der er udarbejdet en fælles forretningsgang vedrørende tilsyn med databehandlere, som forvaltningerne herefter skal implementere.

Der har været fokus på at udarbejde et nyt koncept, der både kunne rumme risikovurdering af it-systemer og den lovpligtige risikovurdering af behandlingen af personoplysninger. Resultatet har været et forbedret koncept i forhold til vurdering af it-systemer, men der foreligger endnu ikke et endeligt godkendt koncept eller vigtigst, en plan for hvordan forvaltningernes ansvar, i forhold til at foretage risikovurderinger af behandlingsprocesser, løftes i tilstrækkelig grad. Det er kritisk og utilfredsstillende for både forvaltningerne, kommunen og ikke mindst for borgerne, da vurderingerne skal sikre et sikkerhedsniveau, der passer til de risici, der er ved forvaltningernes behandling af personoplysninger.

Schrems, tech giganter, Cromebooks m.v.

Den 10. juli 2023 vedtog EU-Kommissionen en tilstrækkelighedsafgørelse med et nyt overførselsgrundlag mellem EU/EØS og USA. Den nye tilstrækkelighedsafgørelse for EU-U.S. Data Privacy Framework etablerer et nyt lovligt overførselsgrundlag for persondata til USA, hvilket er positivt.

Det betyder, at Schrems II problematikken vurderes løst, og at overførsel af personoplysninger til USA isoleret set igen kan ske lovligt.

De grundlæggende krav i GDPR skal stadig efterleves, og det nye overførselsgrundlag løser ikke problematikken vedrørende leverandørernes anvendelse af personoplysninger til egne formål.

Når Københavns Kommune indgår en databehandleraftale med en leverandør, må leverandøren kun behandle personoplysninger til de formål, som Københavns Kommune instruerer leverandøren i jævnfør databehandleraftalen.

Det er en kendt problemstilling, at flere cloud-leverandører anvender personoplysninger til deres egne formål, og således i strid med databehandleraftalens instruks. Det er en stor udfordring, som Københavns Kommune kun vanskeligt kan løse alene, hvilket er et stort problem.

Det er Databeskyttelsesrådgiverens anbefaling at:

- Københavns Kommune inden for de næste 2 år sikrer, at alle kommunens databehandlere ikke anvender kommunens personoplysninger til egne formål.
- Der igangsættes initiativer, der medvirker til at problemstillingen løses i samarbejde med andre store nationale aktører såsom KL, regionerne og statslige myndigheder mv.

Der afventes fortsat en endelig udmelding fra Datatilsynet om anvendelse af data til egne formål hos databehandlere som Google og Amazon Web Services (AWS), jf. blandt andet den verserende sag om brug af Chromebooks i Helsingør Kommune.

Rådgivning, tilsyn, selvejende institutioner samt henvendelser fra Datatilsynet
Vi har i 2023 foretaget tre tilsyn rettet mod alle syv forvaltninger vedrørende:

- Oplysningspligt
- Uddannelse af medarbejdere i IT-Sikkerhed og databeskyttelse
- TV-overvågning

Herudover har vi ydet konkret rådgivning til forvaltningerne og foretaget servicebesøg på decentrale enheder.

Endelig har vi varetaget rollen som DPO for 146 selvejende institutioner som har driftsoverenskomst med Københavns Kommune.

Vi har desuden modtaget og behandlet flere henvendelser fra Datatilsynet.

Alt dette kan du læse mere om i denne rapport og de forvaltningsspecifikke delrapporter.

Fortsat god læselyst!

3. Opfølgning på indsatsområder 2022 (og 2021)

3.1 Governance

I vores statusrapport for 2022 fremhævede vi behovet for at etablere en governance i Københavns Kommune, som kunne skabe klarhed over, hvordan de databeskyttelsesretlige opgaver kunne løses bedst muligt med fokus på at gøre tingene ensartet, højne niveauet samt løse opgaverne på en mere omkostningseffektiv måde.

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

I forlængelse heraf vedtog IT-kredsen (ITK) i februar 2023 fire aktiviteter til at styrke organisering, roller og ansvar. Økonomiforvaltningen har på denne baggrund etableret et "Program for databeskyttelse", som har til formål, at styrke rammerne for en mere effektiv indsats på databeskyttelsesområdet.

Primo 2024 har programmet udarbejdet fire leverancer, som forventes implementeret i 2024:

- Kommissorium for GDPR Forum
- Årshjul for GDPR Forum
- Forankring af modenhedsanalyser
- Snitflader i arbejdet på databeskyttelsesområdet

Kommissorium for GDPR Forum
Der lægges op til, at GDPR Forum skal have en proaktiv rolle i forhold til at identificere og drøfte tværgående forhold af betydning for databeskyttelsesområdet, og at forummet orienterer relevante aktører i Københavns Kommune om eventuelle risici eller manglende overholdelse af databeskyttelsesreglerne.

Hvis GDPR Forum identificerer udfordringer i forhold til efterlevelsen af intern eller ekstern regulering, skal forummet orientere opad i egen forvaltning eller til Digitaliseringschefskredsen (DCK) og ITK. Hvis GDPR Forum identificerer potentielle uhensigtsmæssigheder i kommunens ramme for styring, ansvarsfordelingen og processer, skal GDPR Forum orientere Legal Compliance Forum.

Årshjul
GDPR Forums faste aktiviteter beskrives i øvrigt i "Årshjul for GDPR Forum". Årshjulet kan efter omstændighederne også beskrive aktiviteter, som ikke er forankret i GDPR Forum, men som afspejler kommunens øvrige tilbagevendende aktiviteter på databeskyttelsesområdet. Årshjulet vedligeholdes efter behov af GDPR Forum og skal i øvrigt godkendes af DCK og ITK.

Modenhedsanalyser
Det er i projektgruppen lagt til grund, at forankringen af modenhedsanalyserne (dvs. anvendelsen af modenhedsværktøjet) kan tjene flere formål, herunder:

- Kan sikre, at forvaltningerne løbende arbejder for en højere grad af modenhed i forhold til forpligtelser på databeskyttelsesområdet.
- Kan danne grundlag for tværgående analyser med henblik på at identificere områder, hvor forvaltningerne med fordel kan koordinere indsatserne.
- Kan danne grundlag for en ensartet og sammenlignelig ledelsesrapportering.

Forankringen af modenhedsanalyserne indarbejdes i programmets øvrige leverancer (snitfladedokumentet, årshjulet og kommissorium for GDPR Forum).

Snitfladedokument
For at skabe klarhed omkring de forskellige aktørers roller og ansvar på databeskyttelsesområdet, har der været behov for at udarbejde et snitfladedokument, som præciserer de enkelte funktioners ansvarsområder.

Snitfladedokumentet præciserer på et overordnet og vejledende niveau roller og ansvar i forbindelse med varetagelsen af opgaver på databeskyttelsesområdet. Formålet med dokumentet er, dels at danne et overblik over de beskrivelser, der allerede foreligger i kommunens øvrige dokumenter, dels at præcisere roller og ansvar på områder, hvor der ikke tidligere har været taget udtrykkeligt stilling til dette. Der er således ikke tale om, at de enkelte aktører pålægges nye opgaver eller et øget ansvar.

Forvaltningerne, Koncern IT (KIT) og Databeskyttelsesrådgiveren skal i respekt for de enkelte funktioners ansvarsområder medvirke til, at opgaverne løses hensigtsmæssigt, betryggende og omkostningseffektivt. Dobbeltfunktioner og dobbelt arbejde skal således undgås. Hvis en aktør i en konkret sag oplever tvivl om ansvarsdeling, skal tvivlen afklares fx på et fælles møde med de involverede.

3.2 Implementering af regler og retningslinjer på væsentlige områder

I Årsrapporten for 2022 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.

	Observation	Status 2023
Fortegnelser	Vi har foretaget en stikprøvevis gennemgang af forvaltningernes fortegnelser og i forlængelse heraf meddelt forvaltningerne nogle henstillinger og anbefalinger.	Forvaltningerne har i 2023 afsluttet arbejdet med at udarbejde fortegnelser.
Risikovurderinger	Forvaltningerne foretager stadig ikke de nødvendige risikovurderinger af behandlingsprocesser, og derfor kan forvaltningerne ikke dokumentere, at der træffes passende tekniske og organisatoriske sikkerhedsforanstaltninger ved behandling af personoplysninger.	Der foreligger endnu ikke et endeligt godkendt koncept eller vigtigst, en plan for hvordan forvaltningernes ansvar i forhold til at foretage risikovurderinger af behandlingsprocesser løftes i tilstrækkelig grad.
Konsekvensanalyser	Kommunens konsekvensanalyseværktøj er godkendt.	Forvaltningerne skal anvende værktøjet såfremt der er krav om udarbejdelse af en konsekvensanalyse eksempelvis ved anvendelse af ny teknologi. Herudover identificeres behovet for udarbejdelse af konsekvensanalyser i forbindelse med risikovurderinger af behandlingsprocesser. Denne samlede proces er endnu ikke etableret.
Tilsyn med databehandlere	31. august 2023 har IT-Kredsen godkendt en fællesadministrativ forretningsgang for tilsyn med databehandlere.	Den godkendte forretningsgang er et godt grundlag for, at forvaltningerne kan gennemføre tilstrækkelige tilsynsaktiviteter overfor databehandlere. Det anbefales, at forvaltningerne har fokus på implementering af forretningsgangen i 2024.
Oplysningspligten		Der henvises til de foretagne tilsyn vedrørende Oplysningspligt, i afsnit 4 Tilsyn.

Risikovurderinger af behandlingsprocesser

Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved den dataansvarliges behandlinger af personoplysninger.

Der påhviler således den dataansvarlige en pligt til at identificere de risici, den dataansvarliges behandling udgør for de registrerede og til at sikre, at der indføres passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici.

Kravet i artikel 32 om passende sikkerhed vil normalt indebære, at man som dataansvarlig skal sikre, at oplysninger om registrerede ikke kommer til uvedkommendes kendskab.

Det er endnu ikke lykkedes at få etableret et fælles koncept for risikovurdering af behandlingsprocesser. Der har været fokus på at udarbejde et nyt koncept der både kunne rumme risikovurdering af it-systemer og de tilhørende behandlinger af personoplysninger.

Resultatet har været et forbedret koncept i forhold til vurdering af it-systemerne, men der foreligger endnu ikke et endeligt godkendt koncept eller vigtigst, en plan for hvordan forvaltningernes ansvar i forhold til at foretage risikovurderinger af behandlingsprocesser løftes i tilstrækkelig grad.

Herudover identificeres behov for en konsekvensanalyse i forbindelse med udarbejdelse af risikovurderinger vedrørende behandlingsprocesser. Det er således både kritisk og utilfredsstillende for både forvaltningerne, kommunen og ikke mindst for borgerne i forhold til at sikre et sikkerhedsniveau, der passer til de risici, der er ved forvaltningernes behandlinger af personoplysninger.

4. 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 i forhold til rådgivning og de tilsyn, der er gennemført i 2023.

4.1 Rådgivning

Det seneste år har overvejende været præget af vurderinger i forbindelse med overførsel af personoplysninger til USA, særligt i de tilfælde hvor Københavns Kommune har indgået, eller har ønsket at indgå en aftale med en leverandør, som anvender underleverandører i USA eller andre usikre tredjelande.

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

- Deltagelse i workshops som rådgiver, i forhold til udarbejdelse af et risikovurderingskoncept som rummer en risikovurdering af behandlingsprocesser, set fra den registreredes perspektiv.
- Rådgivning i forbindelse med udarbejdelse af forretningsgang for tilsyn med databehandlere.
- Simplificering af modenhedskonceptet således at konceptet er blevet mere brugervenligt.
- Deltagelse i GDPR-programmet.

Leverandørers behandling til egne formål

Når Københavns Kommune indgår en databehandleraftale med en leverandør, må leverandøren kun behandle personoplysningerne til de formål som Københavns Kommune instruerer leverandøren i.

Det er en kendt problemstilling, at flere cloud-leverandører anvender personoplysninger til deres egne formål, og således behandler personoplysninger, i strid med databehandleraftalens instruks.

Databeskyttelsesrådgiveren har været i dialog med Datatilsynet omkring denne problemstilling, og har på baggrund heraf nogle anbefalinger til Københavns Kommunes fremadrettede håndtering af denne problemstilling.

Københavns Kommune skal sikre, at databehandlere og tilhørende underdatabehandlere, som behandler personoplysninger på kommunens vegne, ikke anvender personoplysningerne til egne formål. Dette fordi kommunen i de fleste tilfælde ikke har hjemmel til at videregive personoplysninger til en leverandør, som behandler disse til egne formål.

Exit-planer

I det tilfælde hvor leverandøren behandler personoplysninger til egne formål, skal der udarbejdes en exit-plan, hvis ikke det er muligt at få leverandøren til at ændre vilkårene i databehandleraftalen.

En exit-plan bør, for hvert system med tilhørende FISKK-id, indeholde en vurdering af nuværende kontraktvilkår, oversigt over, hvornår kontrakten udløber, strategi for markedsafdækning, vurdering af alternative løsninger og en tidsplan for, hvornår kommunen kan udtræde af kontrakten.

Exitplanen skal eksekveres inden for maksimalt to år.

Kommende udbud

Står kommunen overfor et udbud, hvor der ikke vil være nogen bydere, som kan levere en lovlig løsning, kan en ny kontrakt maksimalt løbe i to år. Derfor skal en ny kontrakt udarbejdes, således at kommunen har mulighed for at opsige kontrakten, hvis løsningen ikke er blevet lovliggjort inden da. Perioden skal ikke ses som en stilstandsperiode, og der skal aktivt løbende gøres en indsats for at finde en anden lovlig løsning. Hvis kontrakten er blevet opsagt inden for de to år, grundet en fortsat ulovlig løsning, kan der ikke indgås en ny kontrakt med den pågældende leverandør.

I udbudsmaterialet må det ikke fastsættes som et mindstekrav, at leverandøren ikke må anvende personoplysningerne til egne formål, da leverandøren derved ikke kan anses for konditionsmæssig egnet, og dermed skal diskvalificeres. I stedet bør det anføres som et evalueringskrav, som derved vil favorisere en leverandør, der kan levere en løsning, hvor der ikke sker behandling til egne formål. Samtidig giver det transparens i forhold til hvilke leverandører der anvender data til egne formål.

Uddybende beskrivelse af en leverandørs behandling til egne formål

Siden Datatilsynet nedlagde behandlingsforbud i Helsingør Kommune brug af Chromebooks, som senere blev suspenderet, har der været fokus på databehandlerens brug af personoplysninger til egne formål.

Det følger af forordningen, at alle persondatabehandlinger skal have et lovligt behandlingsgrundlag, som er understøttende for det grundlæggende behandlingsformål.

De store Cloud-udbydere har ofte ugennemsigtige databehandleraftaler, terms of use m.m, hvor de ofte har givet sig selv "lov" til at behandle Københavns Kommunes borgeres personoplysninger til egne formål.

Det kan f.eks. være til markedsføring, produktudvikling, profilering, tracking osv.

Hvis en databehandler, skal have et lovligt grundlag for at behandle personoplysninger til egne formål, skal kommunen lovligt kunne videregive personoplysningerne til dette. Idet kommunerne er offentlige myndigheder, vil behandlingerne ofte være forbundet med myndighedsudøvelse. Lovgivningen tillader derfor ikke, at borgernes personoplysninger behandles til andre formål, end det der følger af den specifikke myndighedsopgave.

Kommunen vil derfor ikke lovligt kunne tillade en databehandler at behandle kommunens personoplysninger til andet, end kommunens egne behandlingsformål.

Der ligger derfor en væsentlig opgave for kommunen, når der kontraheres med en databehandler, i at sikre behandlingssikkerheden, det konkrete aftalegrundlag og instruksen. Dette krav omfatter også databehandlerens underdatabehandlere.

Servicebesøg decentrale enheder i KK

Databeskyttelsesrådgiveren har gentaget succesen fra sidste års servicebesøg, og har som led i vores rådgivnings- og overvågningsforpligtelse, foretaget en række nye servicebesøg hos udvalgte decentrale enheder i Børne- og Ungdomsforvaltningen, Sundheds- og Omsorgsforvaltningen og Socialforvaltningen.

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

I 2023 har vi foretaget i alt 12 servicebesøg. I Sundheds- og Omsorgsforvaltningen har vi besøgt tre centre, hos Socialforvaltningen har vi besøgt en døgnvagt og to dag- og botilbud, og hos Børne- og Ungdomsforvaltningen har vi besøgt seks daginstitutioner.

4.2 Tilsyn

Vi har i 2023 foretaget tre tilsyn i overensstemmelse med den godkendte aktivitetsplan.

Tilsyn med oplysningspligten

Oplysningspligten er en del af registreredes rettigheder som indebærer, at forvaltningerne på eget initiativ skal give de registrerede en række oplysninger, på det tidspunkt hvor kommunen påbegynder indsamling og behandling af personoplysninger om de pågældende.

Vores tilsyn i 2021 på tre forvaltninger viste en utilstrækkelig efterlevelse af oplysningspligten hos to ud af de tre forvaltninger. Vi har derfor gennemført endnu et tilsyn i 2023 og denne gang på alle forvaltninger.

Undersøgelsen viste, at tre ud af syv forvaltninger fortsat ikke efterlever oplysningspligten.

De øvrige fire forvaltninger har alle overblik over, hvor oplysningspligten gør sig gældende. Dog kan der fortsat gives en del anbefalinger til informationsindhold og formidlingsproces, som kun delvist efterleves i forhold til de krav, der stilles hertil.

Tilsyn med uddannelse af medarbejdere

Databeskyttelsesrådgiveren har undersøgt om forvaltningernes uddannelsesplan efterlever kravene i "Forretningscirkulære for Persondatabeskyttelse – Dokumentation og Compliance" pkt. 3.1, og om forvaltningens medarbejdere og ledere får gennemført de obligatoriske uddannelsesmoduler indenfor forvaltningens fastsatte tidsfrist.

Tilsynet er foretaget på baggrund af forvaltningernes fremsendte uddannelsesplan samt en stikprøvekontrol af udvalgte medarbejdere og ledere i kommunens e-læringsuddannelse i plan2learn.

Tilsynet har vist, at forvaltningens uddannelsesplan og uddannelse i al væsentlighed efterlever kravene i "Forretningscirkulære for Persondatabeskyttelse – Dokumentation og Compliance". Dog har tilsynet også vist, at flere ledere på tværs af alle forvaltninger ikke får gennemført modul 7, som er obligatorisk for alle kommunens ledere at gennemføre jf. forvaltningernes uddannelsesplan.

Tilsyn med TV-overvågning

Tv-overvågning anvendes i alle kommunens forvaltninger. Området har de seneste to år haft særlig bevågenhed hos Datatilsynet, ligesom overvågningsteknologi såvel som tv-overvågningsloven har ændret og udviklet sig væsentligt over en relativt kort årrække.

I forbindelse med vores undersøgelse har vi ved tilsynsbesøg i alle forvaltningerne påset, hvorvidt reglerne for behandling af personoplysninger efterleves, når kommunen anvender tv-overvågning. Vores tilsynsbesøg omfattede både borgervendte lokationer såvel som lokationer, der hovedsagelig anvendes af kommunens medarbejdere og samarbejdspartnere.

Vores tilsyn har vist, at der i alle forvaltningerne er, ikke fuldt ud efterlever databeskyttelsesforordningens regler om oplysningspligt, når tv-overvågning anvendes.

Herudover har enkelte af forvaltningerne ikke en fyldestgørende fortegnelse i forhold til deres anvendelse af tv-overvågning.

Overordnet viste undersøgelsen dog også, at der hos de undersøgte lokationer er et acceptabelt niveau af awareness omkring reglerne for videregivelse og sletning af overvågningsoptagelser, samt at anvendelse og opsætning af tv-overvågning foretages på baggrund af saglige og proportionelle hensyn og overvejelser.

5. Henvendelser fra Datatilsynet

Datatilsynet har i løbet af året afsluttet tre tilsyn med Københavns kommune, som ikke har givet anledning væsentlige bemærkninger.

5.1 Afsluttede tilsyn

Arkivloven

Tilsynet blev indledt som et skriftligt tilsyn, som Kultur- og Fritidsforvaltningen behandlede.

Tilsynet omhandlede reglerne i arkivlovens § 34, hvorefter tilladelse efter §§ 31 og 32 og indsigt efter § 39 b kræver samtykke fra Datatilsynet, hvis arkivenheden er afleveret fra en myndighed inden for den offentlige forvaltning og indeholder oplysninger om enkeltpersoners rent private forhold og tidligere behandling af oplysningerne har været omfattet af databeskyttelsesreglerne eller oplysningerne stammer fra et edb-register, der har været ført for den offentlige forvaltning.

Datatilsynet oplyste i deres tilsynsvarsel, at de har kunnet konstatere, at Københavns Kommune havde anmodet Datatilsynet om samtykke få eller ingen gange inden for de seneste to år.

Datatilsynet fandt, på baggrund af Københavns Kommunes besvarelser, ikke grundlag for at foretage sig yderligere og afsluttede tilsynet uden bemærkninger.

Tilsyn tv-overvågning på en sikret døgninstitution

Tilsynet omfattede behandling af personoplysninger i forbindelse med tv-overvågning og blev foretaget som et fysisk tilsynsbesøg. Datatilsynet anmodede forinden det fysiske besøg, om en redegørelse med udgangspunkt i en række spørgsmål om omfang af tv-overvågning, opbevaring af videoovervågningsmateriale, oplysningspligt overfor de registrerede mv.

Datatilsynet havde enkelte bemærkninger til det materiale, som institutionen formidlede til medarbejdere, besøgende mv., som skal oplyse de registrerede om den tv-overvågning, der blev foretaget.

Datatilsynet afsluttede tilsynet uden at foretage sig yderligere.

Undersøgelse om brug af kunstig intelligens løsninger i den offentlige sektor

Datatilsynets formål med spørgeskemaundersøgelsen var at opnå viden om, hvor udbredt brugen af kunstig intelligens-løsninger er blandt offentlige myndigheder, og hvilke juridiske overvejelser myndighederne har gjort sig. Undersøgelsen havde ligeledes til hensigt at italesætte de opmærksomhedspunkter og krav der følger af databeskyttelsesreglerne ved brug af kunstig intelligens.

Undersøgelsen angik hvilke eventuelle løsninger de adspurgte myndigheder har taget i brug og til hvilke formål. Myndighederne blev spurgt om hvilket behandlingsgrundlag, der dannede grundlag for at behandle borgernes personoplysninger ved brug af kunstig intelligens.

Undersøgelsen omfattede 98 kommuner, de fem regioner samt alle ministerier og deres styrelser og institutioner. Undersøgelsen viste, at anvendelsen af kunstig intelligens i vidt omfang bruges til at løse manuelle og tidskrævende opgaver såsom håndtering af fakturaer, sortering af post og journalisering. Derudover viste undersøgelsen, at kunstige intelligens-løsninger anvendes i kontrol- og tilsynsøjemed.

Datatilsynet konkluderede, at brugen af kunstig intelligens endnu ikke er vidt udbredt blandt offentlige myndigheder, og at undersøgelsen indikerede, at myndighederne kan have vanskeligt ved at identificere, hvornår er løsning skal betragtes som kunstig intelligens.

Det er Datatilsynets opfattelse, at behandling af personoplysninger som led i udvikling og drift af AI-løsninger næsten altid vil udløse flere af de kriterier, der er udslagsgivende for, om der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse, forud for behandling.

5.2 Igangværende tilsyn

Undersøgelse vedrørende databeskyttelsesrådgiverens udpegelse og rolle

Som en del af en koordineret undersøgelse i Det Europæiske Databeskyttelsesråd (EDPB), har Datatilsynet fremsendt en spørgeskemaundersøgelse, særligt til databeskyttelsesrådgiveren i landets kommuner.

Formålet med undersøgelsen er, at skabe overblik over, databeskyttelsesrådgiverens arbejde og eventuelle udfordringer forbundet hermed. Spørgerammen indeholder spørgsmål til databeskyttelsesrådgiverens erfaring og viden, hvilke opgaver denne varetager, hvem der rapporteres til m.fl.

Resultatet af rapporten vil blive samlet i en national rapport, hvor Datatilsynet vil evaluere behovet for mere vejledning. Undersøgelsen vil ligeledes blive delt med tilsynsmyndigheder i andre lande i form af en samlet EDPB-rapport.

Undersøgelse om skolebørns brug af Microsoft teams

På baggrund af en klagehenvendelse fra en borger vedrørende Københavns Kommunes registrering af skolebørn i Microsoft Teams, har Datatilsynet indledt en nærmere undersøgelse heraf.

Borgerens klage er afgivet på baggrund af en episode, hvor et skolebarn modtog dødstrusler fra en et andet barn fra en anden skole i kommunen. I den forbindelse har Datatilsynet bedt Københavns Kommune 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.

Tilsyn med AULA

Den 15. oktober 2021 indledte Datatilsynet et tilsyn med 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. Datatilsynet har i forbindelse med tilsynet anmodet kommunen over flere omgange om yderligere dokumentation.

Den 22. maj 2023 henvendte Datatilsynet sig på ny til kommunen på baggrund af en presseomtale om kommunens brug af AULA til journalisering af børnesager. I henvendelsen anmodede Datatilsynet om at få fremsendt Databeskyttelsesrådgiverens tilsynsrapport til vurdering af, om sagen skal indgå i det allerede igangværende tilsyn om kommunens efterlevelse af databeskyttelsesforordningen, om et passende sikkerhedsniveau for kommunens behandlinger i AULA.

Datatilsynet har efterfølgende, af to omgange, anmodet kommunen om yderligere oplysninger i forlængelse af deres henvendelse den 22. maj 2023, hvoraf kommunen senest har besvaret spørgsmål fra Datatilsynet den 21. september 2023.

5.3 Persondatabrud

I perioden 1. oktober 2022 til den 1. oktober 2023 er der blevet registreret 488 indmeldelser om persondatabrud i Københavns Kommune. Sidste år, var dette tal 404.

De hyppigste årsager til persondatabrudende er forsat hændelser, som resulterer i utilsigtet videregivelse på grund af menneskelige fejl.

I 2023 har kommunen ikke modtaget nogen former for kritik i forhold til de indmeldte persondatabrud Datatilsynet har afsluttet.

6. Databeskyttelsesrådgiverfunktionen for selvejende institutioner med driftsoverenskomst

Borgerrepræsentationen vedtog 11. oktober 2018, at tilbyde de selvejende institutioner som har driftsoverenskomst med KK, vederlagsfrit at få kommunens databeskyttelsesrådgiver som institutionens databeskyttelsesrådgiver.

Pr. 1. oktober 2023 er 146 selvejende institutioner fordelt på 110 daginstitutioner, 12 sociale institutioner og 24 plejehjem, omfattet af ordningen.

Den primære aktivitet i 2023 har været tilsyn på udvalgte institutioner og institutioner, der ikke har søgt eller modtaget DPO's rådgivning indenfor de sidste 12 måneder.

Resultatet af vores tilsyn viser, at de større institutioner typisk har et tilfredsstillende niveau på databeskyttelsesområdet og har implementeret institutionsspecifikke retningslinjer, medarbejderuddannelse og ledelseskontrol.

Mindre institutioner har i flere tilfælde vanskeligt ved at opretholde et tilstrækkeligt databeskyttelsesniveau. Dette på trods af, at vi har en løbende og meget intensiv formidling og rådgivning, ligesom vi stiller alle tænkelige værktøjer til rådighed for alle institutionerne. Ved alle tilsyn modtager ledelsen et notat med resultatet af vores tilsyn.

Når et tilsyn viser, at en institution ikke har et tilstrækkeligt niveau på databeskyttelsesområdet, udarbejdes notet både til ledelsen og bestyrelsen med konkrete henstillinger og anbefalinger. Herudover planlægges rådgivning eller tilsyn i forhold til at påse, at institutionerne har det nødvendige fokus på at sikre et tilstrækkeligt databeskyttelsesniveau

Generelt ser vi udfordringer i forhold til databeskyttelsen, når institutioner skifter leder eller GDPR-ansvarlig som typisk kan henføres til manglende overdragelse fra gammel til ny leder. Vi modtager sjældent oplysninger om lederskift. Hvis vi bliver bekendt med lederskift, kontakter vi institutionen, hvilket i de fleste tilfælde giver anledning til at institutionen skal genimplementeres.

Vi har blandt andet gennemført følgende aktiviteter i 2023:

- 38 fysiske og skriftlige tilsyn
- 77 rådgivningsopgaver, hvor 14 opgaver har været introduktion og implementering i forbindelse med leverskifte
- 11 databrud, hvor der er søgt rådgivning i forbindelse med håndtering og anmeldelse til Datatilsynet
- 2 undervisningswebinarer
- On-boarding af 2 nye institutioner.

Erfaringerne fra 2023 bliver anvendt som grundlag for vores aktiviteter i 2024, hvor vi igen vil screene alle institutionerne i forhold til deres databeskyttelsesniveau. Herudover vil vi øge tilsynsaktiviteterne, da der er vores vurdering af det virker motiverende hos institutionerne.

Institutioner uden for ordningen

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

Af de 27 institutioner, som har valgt ikke at være omfattet DPO-ordningen, kan 4 henføres til SOF og 23 henføres til BUF. Alle selvejende institutioner i SUF er omfattet ordningen.

SOF oplyser, at der reelt er en institution der har valgt ikke at tilslutte sig ordningen. De tre andre er i proces.

BUF oplyser, at én nyoprettet selvejende institution, ønsker at være omfattet ordningen men forvaltningen gør ikke noget aktivt for at udbrede kendskabet til DPO-ordningen til de selvejende institutioner. Dog gøres institutionerne opmærksom på DPO-ordningen, hvis de kontaktes i anden anledning.

For de resterende ikke-tilmeldte institutioner vil BUF overveje, om der skal foretages en intern opfølgning for at vurdere deres complianceniveau.

Vi anbefaler at BUF søger at få flere institutioner ind i ordningen for at minimere omkostningerne både i forvaltningen og hos institutionerne.

København, den 24. januar 2024

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