



Bilag 2

Kodeks for kunstig intelligens og databeskyttelse

15-08-2022

Baggrund

Økonomiudvalget i Københavns Kommunes vedtog d.18. februar 2020 "Kodeks for anvendelse af kunstig intelligens". Sammen med den eksisterende lovgivning sætter kodekset rammerne for anvendelse af kunstig intelligens i København. I notatet redegøres for, hvordan innovationscasen understøtter kodekset samt de generelle retningslinjer omkring databeskyttelse i KK.

Sagsnummer i F2
2022 - 11808

Dokumentnummer i F2
1752614

Sagsnummer i eDoc
2022-0255546

Kodeks for kunstig intelligens

Kodekset består af fem mål og fem principper. De fem mål i kodeks for kunstig intelligens er:

1. Der skal være tillid til kommunens brug af kunstig intelligens
2. Kunstig intelligens skal bidrage til bedre service for borgere og virksomheder
3. Kunstig intelligens skal frigive ressourcer til kernevelfærden
4. Kunstig intelligens skal være en støtte til fagligheden
5. Kodekset skal følge erfaringer og udvikling i lovgivningen

Teknik- og Miljøforvaltningen vurderer, at brug af videobaseret sensorteknologi og kunstig intelligens understøtter målene i kodekset. I forhold til mål om tillid har forvaltningen lægt vægt på en grundig markedsafdækning og analyse samt et eksplicit fokus på håndtering af databeskyttelse. Pilotprojektets brug af sensorer og kunstig intelligens/algoritmer skal herudover bidrage til, at forvaltningen på sigt kan frigøre ressourcer og levere en bedre opgaveløsning på vejområdet.

Innovationsprojektet brug af sensorteknologi taler ligeledes ind i de fem principper for kodekset:

Princip 1: Ansvarlighed

Ansvarlighed indebærer, at der altid tages organisatorisk og ledelsesmæssigt ansvar for arbejdet, der udføres af teknologien. I innovationscasen udnyttes teknologien som hjælpeværktøj til at identificere vejskader, hvorefter beslutninger om indsatser tages i ledelse og organisation. Ligesom teknologiens tilstandsvurderinger

Stab
Islands Brygge 37
2300 København S

EAN-nummer
5798009809452

løbende sammenholdes med fagligt kompetente medarbejdes inspektion.

Princip 2 - Borgernes retssikkerhed

Forvaltningen har fået gennemført en analyse af EY med en markedsafdækning af sensorteknologier og en vurdering af videobaseret sensorteknologi. Analysen belyser, at en videobaseret sensorteknologi er GDPR-compliant.

TMF vil herudover i valg af leverandør i pilotprojekt kigge på den samlede håndtering af dataprocesser og teknisk setup og ud fra en samlet risikovurdering vælge leverandør. I valget vil forvaltningen lægge vægt på, at leverandøren lægger vægt på privacy by design. Fx ved at maskering af personhenførbare data sker så tidligt og sikkert så muligt.

Princip 3 og 4 omhandler hhv. lighed og retfærdighed samt gennemsigtighed i forhold til afgørelser vedr. borgerne. I pilotprojektet anvendes ikke personhenførbare data til opgaveløsningen, og der træffes ikke beslutninger omkring borgere. De 2 principper er derfor ikke relevante.

Princip 5 - cybersikkerhed

Princippet lægger vægt på, at såvel data som teknologi beskyttes. Innovationscasens aktører, leverandører og medarbejdere vil alle være omfattet af kommunens generelle sikkerhedskrav til såvel håndtering som opbevaring af - og adgang til data og den tekniske løsning.

Databeskyttelse (GDPR) og privacy i forhold til innovationscasen

Innovationscasen betyder, at der anvendes videobaseret sensorteknologi i dele af det offentlige rum i Københavns Kommune. Det er relevant i forhold til princip 2 ovenfor om hensynet til beskyttelse af borgernes privatliv, også kaldet privacy. Teknik- og Miljøforvaltningen vil derfor stille krav om, at den teknologi, der anvendes, skal maskere og/eller slette personhenførbare data (persondata), som evt. måtte blive optaget v. indsamling af rådata. Det betyder, at håndteringen af persondata i casen udelukkende består i, at sådanne data hurtigst muligt skal fjernes i processen.

I det omfang fjernelsen af sådanne data sker allerede umiddelbar sammenhæng med indsamlingsfasen, er der tale om databeskyttelse gennem design efter art. 25 i GDPR, også kaldet privacy by design. Dette indebærer ifølge forordningen, at der allerede fra tidspunktet, hvor midlerne for behandlingen fastlægges (f.eks. kamerateknologi med video), skal gennemføres passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på at sikre en effektiv implementering af de grundlæggende databeskyttelsesprincipper, det er f.eks. lovlighed, rimelighed og gennemsigtighed.

TMF ønsker at købe en løsning af en leverandør, der opfylder ovennævnte krav om helt at fjerne persondata. For at sikre at det også er tilfældet i praksis udfører forvaltningen en risikovurdering af løsningen i samarbejde med leverandøren. Der er tale om en risikovurdering af den tekniske løsning med inddragelse af databeskyttelseshensyn. Først når persondata er fjernet vil optagelsen blive lagret og anvendt i kommunens vejtilsyn. På baggrund af resultatet af risikovurderingen vil det blive vurderet, om der skal foretages en konsekvensanalyse af behandlingen efter GDPR art. 35.

Da formålet med løsningen er, at forvaltningen kan føre vejtilsyn og ikke at behandle persondata i den sammenhæng, vil forvaltningen ikke have noget dataansvar.