



Til Teknik- og Miljøudvalget

01-12-2014

Sagsnr.
2014-0265726

Bilag: Beskyttelse af borgernes privatliv i den intelligente by

Dokumentnr.
2014-0265726-6

Baggrund

Notatet er udformet på baggrund af sagen om frigivelse af midler til Smart City, som behandles på Teknik- og Miljøudvalget d. 26. januar 2015. SF har rejst nogle spørgsmål angående beskyttelse af borgernes privatliv i den intelligente by og har henvist til artikler, kronikker mv. omhandlende smart city og borgernes privatliv. Forvaltningen indsamler data efter gældende dansk lovgivning og sikrer at data anonymiseres på laveste niveau, så det ikke er muligt at følge eller identificere navngivne personer ud fra de oplysninger der registreres. Denne praksis følges i dag, og vil også gælde fremover.

Sagsbehandler
Rikke Margrethe Møller
Gram-Hansen

I forhold til projektet om et smart city testområde og ITS udbuddet, er det ligeledes et krav at alle løsninger overholder gældende lovgivning – og derudover følger vores egne (kommende) guidelines for indsamling af data og smart city løsninger.

Den intelligente by

Udviklingen i digitale teknologier og datadrevne byløsninger, også kaldet smart city teknologier, giver nye muligheder for, at kommunen kan løse sine opgaver på en mere effektiv måde, få et bedre grundlag for at træffe beslutninger indenfor planlægning og drift af forvaltningens fagområder og give en bedre service til borgerne. Smart city løsninger er i høj grad baseret på indsamling og anvendelse af data, men der er i vid udstrækning ikke tale om indsamling af personhenførbare data. Dilemmaet er dog, at jo mere detaljerede data er, jo bedre en planlægning eller service kan man udvikle på baggrund deraf, så de nye muligheder stiller også nye krav til, hvordan vi kan sikre beskyttelse af borgernes privatliv, digitale rettigheder og datasikkerhed – og hvordan vi formidler dette til borgere, erhvervsliv og samarbejdspartnere.

Teknologisk beskyttelse af privatlivet

Al indsamling af data i byrummet skal ske indenfor rammerne af gældende lovgivning. Der er stor forskel på de typer af data, der indsamles i datadrevne byløsninger alt efter hvilken teknologi, der anvendes. Der findes teknologier, der er smarte, men som ikke indsamler personhenførbare data. Eksempelvis kan et trafikamera, der anvendes til trafikstyring, analysere billederne direkte i kameraet, således at det kun videresender data om antal køretøjer på et givent tidspunkt. Et andet eksempel er sensorer eller kameraer, der registrerer om en parkeringsplads er ledig eller ej, men som ikke registrerer *hvem* der bruger pladsen. Privatlivsbeskyttelse er tænkt ind i disse løsninger fra start, hvilket kaldes *privacy by design*. De data vi indsamler i

byrummet er således ikke direkte henførbare til bestemte personer, men det er stadig nødvendigt at sikre privatlivsbeskyttelse i forhold til hver enkelt løsning.

Persondataloven

Indsamling af data, som kan henføres til en identificeret eller identificerbar person, hører ind under Persondatalovens strengeste bestemmelser. Persondataloven sætter rammerne for hvem og hvornår man må indsamle og behandle persondata:

Generelt skal der være et sagligt formål med indsamlingen, og indsamlingen skal ske indenfor myndighedens naturlige fagområde, og skal være i samfundets interesse. Smart city teknologier anvendes netop til at forbedre kommunens opgaveløsning i de forskellige fagområder, eksempelvis trafikstyring, skraldeindsamling, parkeringssensorer, skybrudssikring mv., og for at sikre en bedre service til Københavnerne.

Persondataloven tilsiger, at der ikke må indsamles mere data om borgerne end højst nødvendigt i forhold til formålet, og at data skal slettes eller anonymiseres, når der ikke længere er behov for dem i en direkte identificerbar form. Persondataloven muliggør også behandling af persondata ved udtrykkeligt samtykke, hvilket f.eks. kan ske, hvis kommunen eller andre parter udvikler en app, som giver borgeren en bestemt service, der forudsætter at borgeren skal acceptere indsamling af data. Eksempelvis kræver en app til rejseplanlægning med brugen af GPS, at man accepterer, at leverandøren registrerer, hvor man opholder sig, for at kunne vise ruten til destinationen.

EU-Cookiedirektivet og device fingerprinting

Erhvervsstyrelsen har slået fast, at EU's cookiedirektiv også gælder device fingerprinting dvs. sporingsteknologier. Hvad det konkret betyder, vil styrelsen udarbejde en udspecificeret vejledning for. Såfremt Erhvervsstyrelsen og andre lovgivende myndigheder slår fast, at det ikke er lovligt f. eks. at gemme krypterede MAC og BlueTooth adresser for at måle rejsetider, så vil København ikke bruge disse teknologier – med mindre brugerne på forhånd har givet et aktivt frivilligt tilsagn, om at vi må gøre det, ligesom i eksemplet med en app til rejseplanlægning.

Datasikkerhed

Persondataloven stiller også krav til håndteringen af persondata, så personoplysninger ikke kan komme til uvedkommendes kendskab. I København vil det være hensigtsmæssigt at anskue håndtering af data bredere, så det angår alle data kommunen indsamler i byrummet, og ikke kun de personfølsomme. Det kan eksempelvis være ved at etablere retningslinjer, så data kun må opbevares på dansk grund og ved at udpege dataansvarlige i forvaltningen.

Principper for privatlivsbeskyttelse

Faste retningslinjer fra start kan sikre borgernes privatliv og digitale rettigheder i udrulning af datadrevne løsninger på tværs af kommunen. *Privacy by design* principper er således en metode kommunen kan anvende til at sikre privatlivsbeskyttelse. Det vil være et vigtigt redskab for medarbejdere, leverandører og samarbejdspartnere, så det er klart for alle, hvor kommunen står. Et eksempel på hvordan principper kan udformes findes i bilag til ITS handlingsplanen, *se vedlagte notat*. I Budget 2013 (BR 4. oktober 2012) (A, B, F, I og Ø) afsatte Borgerrepræsentationen 60 mio. kr. til ITS (Intelligente Transport Systemer), som er et initiativ under KBH 2025 Klimaplanen.

For at sikre, at kommunen formidler overfor omverdenen, hvordan vi tager borgernes privatliv, personlige frihed og inddragelse seriøst i anvendelsen af nye teknologier og datadrevne løsninger i byrummet, kunne principperne udvikles til et charter, eksempelvis kaldet 'Copenhagen Charter for Privacy and Digital Rights in Smart City Solutions'. Det er vigtigt at kommunikere klart om, hvordan vi håndterer disse spørgsmål, så borgerne kan føle sig trygge i deres by. Et initiativ som dette vil også være med til at gøre København til en førende by på området, som andre hovedstæder og virksomheder vil kigge til for en samfundsansvarlig smart city model.

Deltagelse i offentlig debat

Ved siden af udvikling af klare retningslinjer for anvendelsen af smart city teknologier, er der en offentlig debat om privatliv og overvågning, som Københavns Kommune vil indgå aktivt i. Copenhagen Solutions Lab vil bl.a. bidrage til en informeret debat med borgerne, og har derfor dialog med Dansk Arkitektur Center om et eller flere debatarrangementer om privatliv og smart city, fx i forbindelse med deres udstilling Den Intelligente By senere på året og i forbindelse med Folkemødet til sommer.

Anbefalinger fra eksperter

For at sikre at kommunen fremadrettet griber nye datadrevne teknologier og privatlivsbeskyttelse rigtigt an, så vi udnytter de gode muligheder i smart city løsninger uden at gå på kompromis med lovgivning og privatlivsbeskyttelse, vil Byens Anvendelse og Copenhagen Solutions Lab nedsætte et ekspertpanel. Det er tanken at sammensætte et panel af eksperter der repræsenterer forskellige kompetencer indenfor teknologi, jura, etik, samfundsforhold og erhvervsliv. De skal komme med deres anbefalinger til, hvordan vi konkret kan sikre, at København bliver førende som en intelligent by, som beskytter borgernes privatliv, baseret på internationale erfaringer, og med inddragelse af relevante interesseorganisationer. Forvaltningen har ikke inviteret deltagere endnu.

Deres anbefalinger skal vise vejen for det videre arbejde med privatlivsbeskyttelse i den intelligente by, hvilket der vil blive søgt midler til at fortsætte og styrke i Budget 2016.

Smart city testområdet i Indre By

I forhold til det konkrete projekt med at oprette et smart city testområde i Indre By, vil der ikke blive opsamlet datatyper til trafikoptimering fra smart phones og andet elektronisk udstyr, som vi ikke allerede i dag indsamler i byen. Byens Anvendelse har for eksempel indkøbt og opsat udstyr i byen til indsamling af data fra smart phones til monitorering af trafikken i København. Samme teknologi benyttes i øvrigt i mange andre danske og internationale byer til samme formål; trafikoptimering. Disse data krypteres og anonymiseres, så man ikke kan finde tilbage til en bestemt telefon og dermed ejerens bevægelser.

Konkret hvordan teknologien fungerer og hvordan det sikres, at teknologien ikke kan misbruges f.eks. ved at forsøge at gøre data personhenførbare, er beskrevet i det førnævnte bilag til ITS handlingsplanen. Konsortier som byder på kommunens kommende ITS udbud forventes, at levere forslag om yderligere udrulning af denne type teknologi i byrummet bl.a. for at undgå at udrulle dyrere kamera baserede teknologier.

Copenhagen Connecting

Copenhagen Connecting er et idékatalog over mulige smart city løsninger, baseret på input fra borgere, universiteter, virksomheder og fagenheder i kommunen. Det er ikke politisk behandlet.

Ideerne er offentligt tilgængelige på hjemmesiden, i uredigeret og uzensureret form i et online regneark som automatisk opdateres når der indsendes nye forslag, som læserne samme sted opfordres til at indsende. Ideerne skal være inspiration til, hvad man kan gøre for at løse forskellige udfordringer for byen og bud på prioritering af indsatsområder i KK's Smart city arbejde.

Copenhagen Connecting indeholder udover et idékatalog, også en analyse af, hvad gevinsterne for samfundet er ved forskellige smart city teknologier. Det er værdifulde informationer hvis ideerne på et tidspunkt skal omsættes til handlinger, fordi de viser borgere og beslutningstagere, hvilke initiativer, der vil kunne gavne samfundet mest i forhold til, hvor de største gevinster er indenfor fx CO₂ reduktion som en del af KK's målsætning om at blive CO₂ neutral i 2025.

Smart city nedefra og op

I SF's henvendelse til forvaltningen nævnes Ministeriet for By, Bolig og Landdistrikters publikation "Fremtidens Byer er digitale og

menneskelige” som indeholdende gode eksempler på nedefra og op initiativer. Flere af Københavns Kommunes initiativer fremgår af publikationen, eksempelvis Copenhagen Connecting og Copenhagen Solutions Lab. Et andet af initiativerne i publikationen er Københavns nedsættelse af Projektrådet for Smart City, som samler direktørerne fra Økonomiforvaltningen, Teknik- og Miljøforvaltningen, Koncernservice og Kultur- og Fritidsforvaltningen, fordi den intelligente by skal tænke løsninger og udfordringer på tværs. Københavns Kommune har også flere af de andre nævnte initiativer, eksempelvis Giv et præj-løsninger, og, ligesom Aarhus, en Open Data Portal, data.kk.dk, så borgere, iværksættere og virksomheder kan være med til at skabe fremtidens services til kommune og borgere. De ikke-personfølsomme data kommunen indsamler kan her stilles til rådighed for interesserede, hvilket skaber åbenhed om forvaltningens arbejde og mulighed for at genanvende kommunens data i nye løsninger, der skaber vækst og viden.

Bilag: Beskyttelse af borgeres privatliv i den intelligente by

En række af de tiltag der er beskrevet i ITS handlingsplanen, baserer sig på indsamling, behandling og anvendelse af trafikdata. Det stiller krav til en forsvarlig håndtering af data.

Persondataloven

Indsamlingen af trafikdata vil ske under fuldt hensyntagen til persondataloven. Som udgangspunkt udgør anonymiserede trafikdata ikke personoplysninger, da de netop er anonyme.

Hvis nogle datatyper kan anses for persondata, giver loven mulighed for, at offentlige myndigheder kan indsamle og behandle disse, fx hvis behandlingen er nødvendig for at kunne udføre en opgave i samfundets interesse. Indsamling af trafikdata har et klart fagligt formål, og sker allerede i stor udstrækning mange andre steder i landet. Københavns Kommune indsamler og behandle desuden allerede store mængder persondata på andre områder end trafik.

Principper

De konkrete arbejdsgange og løsninger vil blive præciseret som del af det kommende ITS udbud, men vil tage udgangspunkt i følgende principper:

- Der indsamles kun data med et klart sagligt formål.
- Data gemmes kun i anonymiseret form.
- Data gemmes ikke i længere tid end nødvendigt.
- Identifikationsnumre på digitale enheder, opsamlet via fx WIFI/Bluetooth/RFID, gemmes kun i krypteret form.
- Indsamling af data fra apps på smartphones vil kun ske efter samtykke fra brugeren.
- Kun relevante medarbejdere får adgang til rådata, dvs. data der ikke er aggregerede gennemsnitsværdier.
- Der vil være fuld åbenhed om, hvilke data der indsamles og hvordan de anvendes, så borgerne ikke misforstår formålet og føler sig overvågede.
- Der foretages regelmæssige audits af en ekstern partner for at sikre, at forvaltningen overholder 'best practices' på området.

Eksempler på datakilder

Nedenstående illustrerer, hvilke type data forskellige teknologier indsamler. Der er ikke tale om en udtømmende liste.

Spoler

Anvendes bl.a. til trafikstyring. Spoler i vejen kan ikke identificere personer eller køretøjer, men leverer kun data om antal og tidspunkt for køretøjer, der passerer.

Bilag til indstilling om
ITS handlingsplan
behandlet på TMU
d. 1.12. 2014

Sagsnr.
2014-0265726

Dokumentnr.
2014-0265726-6

Sagsbehandler
Rikke Margrethe Møller

Trafikkameraer

Trafikkameraer, der anvendes til trafikstyring, videregiver ikke billeder eller video, men analyserer billederne lokalt i kameraet og videregiver kun data om antal og tidspunkt for køretøjer, der passerer.

Trafikkameraer, der bruges til at vurdere den trafikale situation på udvalgte steder i byen, sender video til forvaltningens systemer via sikre forbindelser, så udvalgte medarbejdere kan se live video på en skærm, men video gemmes ikke, og kan ikke tilgås af eksterne.

WIFI, BlueTooth og RFID antenner

Smartphones, headsets og andet digitalt udstyr, med trådløst netværk slået til, udsender løbende et unikt ID. Små RFID tags udsender også et unikt ID, og kan monteres på fx cykler eller genstande.

ID'erne kan aflæses, når man passerer opsatte antenner. Hvis ID'et gemmes, kan man følge enheden fra antenne til antenne og derved beregne fx rejsetider og rejsemønstre.

ID'erne kan ikke umiddelbart knyttes til en person eller genstand, da der ikke findes et centralt register over dem. Derudover vil de kun blive gemt i krypteret form.

Apps

Smartphones indeholder en række sensorer, bl.a. GPS og accelerometer. Data fra disse sensorer kan anvendes til en lang række formål indenfor ITS og trafikledelse. Fx kan GPS data give oplysning om antal stop og ventetider i enkelte kryds.

Data fra smartphones vil kun blive indsamlet med brugerens samtykke.

Implementering

Principperne, der er beskrevet i dette notat, vil blive indarbejdet i det kommende ITS udbud, så det sikres, at de ITS systemer, der indkøbes og implementeres, følger al gældende lovgivning og sikrer borgerne anonymitet og åbenhed.

Arbejdet med Smart City andetsteds i TMF er også i høj grad baseret på data. Der er derfor en dialog med Copenhagen Solutions Lab omkring etablering af et sæt fælles retningslinjer for indsamling og behandling af data.