GDPR Compliance i Smart City projekter

Eirik Oterholm Nielsen[1] | Christian D. Jensen[1]

[1] DTU Compute, Sektion for Cybersikkerhed

Keywords: Smart City, GDPR, Compliance, Hjemmel

Abstract

Der er stor udvikling i anvendelsen af Smart City teknologier i Danmark. Sensorer sættes op flere steder i byrummet for at indsamle data, der kan forbedre den kommunale service – endda på tværs af kommunegrænser. Men hvilke data må kommunerne indsamle og opbevare? Hvilke må deles med andre og hvordan? Og hvordan sikres persondata rent praktisk imod misbrug?

I SAnD-projektet (Sikker og Anvendt Data) skriver vi en håndbog der diskuterer disse emner. Det handler om at vide hvem, der må tilgå hvilket data, i hvilke situationer og med hvilken hjemmel.

Indsamling, opbevaring og brug af data skal også være gennemsigtig for borgeren, så borgerne kan se hvordan og hvorfor, deres data bliver brugt. Derigennem kan der skabes større tillid og velvilje til Smart City-projekter.

1 | Introduktion

Der er en kæmpe udvikling i gang indenfor Internet of Things (IoT). Teknologien har gjort det billigere at indsamle data fra sensorer i bybilledet. Batterier varer længere, så de skal ikke skiftes lige ofte, og det er blevet mere effektivt at kommunikere data trådløst med nye netværksteknologier, som f.eks. Bluetooth Low Energy (BLE), NB-IoT, Sigfox og LoRaWAN. Dette giver nogle spændende muligheder for at udvikle byer med Smart City teknologier. Om det drejer sig om trafikplanlægning eller -styring, spildevandshåndtering, håndtering af regnvand i forbindelse med skybrud eller forbedring af indeklima i skoler, så er der stort potentiale i at sætte sensorer op for at finde ud af, hvordan byen kan forbedres. Der er dog en tilsvarende stor risiko for, at disse data kan blive misbrugt. Et kamera, der tæller biler, kan misbruges til at overvåge adfærd på gaden, og sensoren, der tjekker indeklima på et kontor, kan bruges til at bekræfte, hvornår kontorets ejer er til stede. Persondataforordningen (GDPR) skal forhindre misbrug af data, bl.a. gennem store bøder til dem, der overtræder reglerne. Den er dog ikke godt forstået af mange kommunale medarbejdere, så der kan opstå en berøringsangst over for indsamling og brug af data, hvilket vil bremse udviklingen af Smart City. I det efterfølgende giver vi en kort gennemgang af flere GDPR-principper og diskuterer, hvordan de påvirker et Smart City projekt. Dermed håber vi at kunne skære igennem tågen og bane vej for udvikling af smarte byer i Danmark.

Hvad har den kommunale medarbejder behov for at vide, når de skal påbegynde et Smart City projekt? De skal først og fremmest identificere, hvilke data der indsamles og afgøre om disse data kan betragtes som persondata. Hvis data ikke kan betragtes som persondata, stiller GDPR ingen forhindringer i vejen for projektet (se dog den efterfølgende diskussion af, hvordan man afgør om data er persondata i sektion 3). Hvis data kan betragtes som persondata, skal der afgøres hvilken hjemmel, der er til at indsamle disse data. Hvis man ikke kan finde hjemmel, må data ikke indsamles. Baseret

på hvilken hjemmel man har til at indsamle persondata, så har registrerede personer forskellige rettigheder, der skal tages hensyn til. Det er især vigtigt, når en offentlig myndighed indsamler personoplysninger, at det er klart, hvad disse data skal bruges til, dvs. med hvilken hjemmel de indsamles, og til hvilke formål de bliver brugt. Yderligere skal det være klart, hvordan data bliver anonymiseret eller beriget, så borgeren og andre, der efterprøver lovligheden (Eng. "compliance"), kan verificere om data bliver korrekt behandlet. Ved at gennemgå den håndbog, der udarbejdes af SAnD projektet, vil læseren møde disse problemstillinger ved Smart City udvikling, og få værktøjer til at håndtere dem.

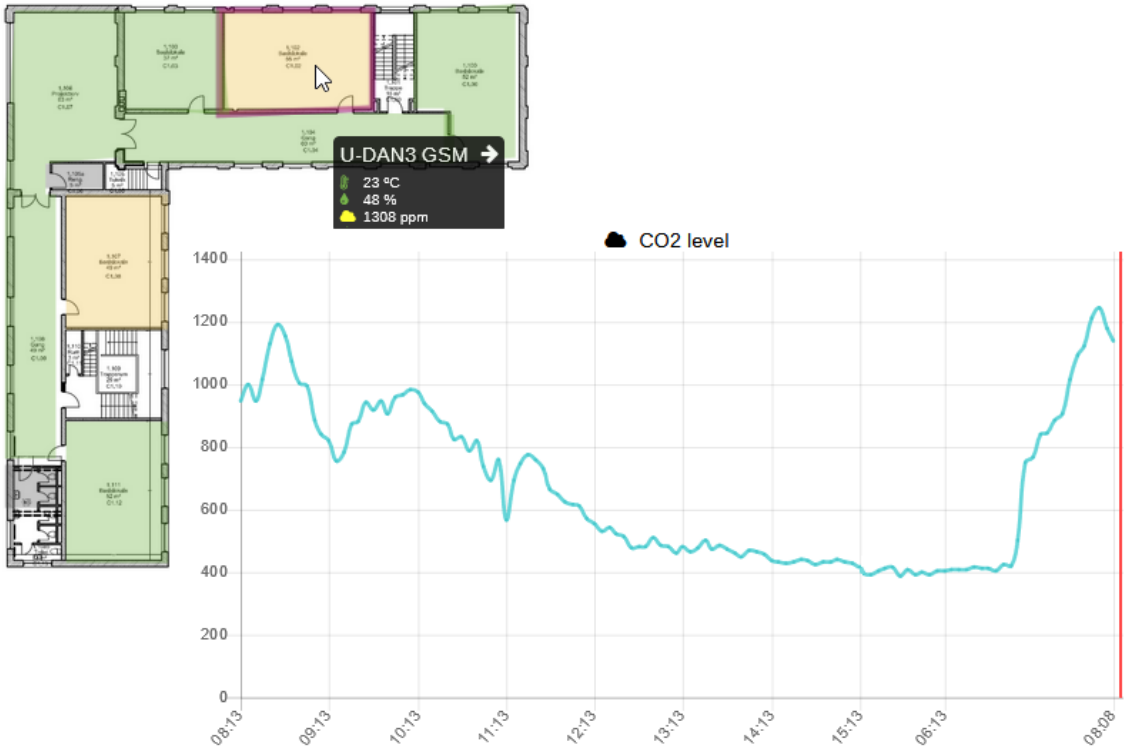
Vi er ikke juridiske eksperter, men har primært styr på datasikkerhed, så tag vores juridiske vurderinger med et gran salt og konsulter egne jurister, inden projekter iværksættes. Vi håber dog, at denne artikel kan hjælpe med at kvalificere diskussioner med beslutningstagere og jurister, så nye smart city projekter kan iværksættes på et holdbart etisk og juridisk grundlag.

2 | Climify: En Case Study

For at demonstrere metoderne beskrevet i artiklen, har vi valgt at tage udgangspunkt i Climify projektet som case. Det er et projekt udviklet på DTU Compute i sektionen DynSys i samarbejde med flere kommuner. Projektet udvikler hjemmesiden www.climify.com, et dataindsamlings- og visualiseringsværktøj, der lader skoler indsamle indeklimadata fra forskellige sensorer og præsentere disse på en overskuelig måde. I denne case study fokuserer vi på indsamling og behandling af følgende data:

Støjniveau Temperatur CO2 Luftfugtighed

Disse bliver indsamlet fra rum i skolebygninger hvert femte minut, hvilket giver et øjebliksbillede af indeklimaet. Data bliver præsenteret på en gulvplan, så det er nemt at se indeklima i et specifikt lokale på et givet tidspunkt, samt i en graf der giver bedre oversigt over udviklingen over tid af indeklimaværdier i et givet lokale. Begge visualiseringsformer er illustreret i figur 1.



Figur 1: Climify indeklima graf og gulvplan

Projektets primære mål er at give skoler og kommuner et værktøj, der giver et præcist overblik over indeklima i skolerne. Dermed kan de identificere lokaler, hvor indeklima ikke er godt nok under undervisning, sætte initiativer i gang for at forbedre situationen og evaluere effekten af disse initiativer. Dette kunne være initiativer som bedre isolation, ventilation eller undervisning i indeklima hygiejne. Et sekundært mål i projektet er demokratisering af indeklima. Det er godt for studerende og undervisere at kunne se at deres undervisningslokaler har et godt indeklima, samt at se effekten af at lufte ud eller andre handlinger. For yderligere information vedrørende projektet, kontakt Davide Cali på dcal@dtu.dk.

3 | Hvordan afgøres om indsamlet data er personoplysninger

Datatilsynet definerer data som personoplysninger, hvis de kan relateres til en fysisk person. Det er også tilfældet, hvis dette opnås ved at kombinere med andre data, således at det samlede billede relateres til en fysisk person. Ifølge Datatilsynet er det ligegyldigt, om den enkelte person, der har adgang til data, kan henføre disse til en fysisk person, så længe at der findes nogen, der kan gøre det, så skal data betragtes som personoplysning.

Hvordan afgør vi så, om data kan relateres til en fysisk person? Vi definerer to simple kriterier, der kan hjælpe med at besvare dette spørgsmål.

Det første kriterie bygger på, om data påvirkes af mennesker, hvis data er uafhængige af menneskelige aktiviteter, er der ikke tale om personoplysninger. F.eks. vil et udendørs termometer i de fleste situationer ikke have noget med en fysisk person at gøre. Temperaturen udenfor er den samme, så længe at sensoren ikke bliver sat op foran en terrassevarmer eller lignende. Indendørs forholder det sig anderledes, fordi temperaturen i et lokale kan variere som følge af menneskelig

aktivitet. Det kan være et lille gymnastikhold, der opvarmer et underdimensioneret lokale, eller en frysende medarbejder der skruer op for radiatoren.

Det andet kriterie er at vurdere om det vil være muligt at identificere enkeltpersoner gennem sensordata. Hvis sensoren er sat op, sådan at en enkeltpersons aktiviteter har en betydelig påvirkning på sensordata, så indsamles der personoplysninger om denne person. Dette gælder også, hvis der indsamles generelle oplysninger, der påvirkes af en gruppen som helhed, men hvor en identificerbar person har betydende indflydelse på gruppens adfærd, såsom en kaptajn på et skib, en sergent i en infanterigruppe eller en lærer i en skoleklasse.

Hvis vi efter gennemgang af disse kriterier kan sige, at de indsamlede data ikke kan relateres til et enkelt individ, så er det sandsynligt vis ikke personoplysning. Vi bemærker dog, at når der indsamles tilstrækkeligt store mængder præcise data, er der altid risiko for, at der findes nogen, der kan udføre en statistisk analyse, der viser, hvordan enkeltpersoner påvirker variationer i data; hvis dette er tilfældet, udgør data også en personoplysning. Dette kræver dog, at den statistiske analyse er nem at udføre, og kommuner vil formegentlig ikke blive stillet til ansvar for avancerede statistiske dataanalyser, de ikke kan forventes at kende til. (GDPR Betragtning 26)

3.1. Er data indsamlet i Climify personoplysninger?

For at illustrere brugen af de tre kriterier, ser vi på de data, vi indsamler i Climify projektet. For at holde diskussionen kort, ser vi kun på måling af støjniveau i klasselokaler.

Ved at anvende det første kriterie, ser vi, at støjniveau i et lokale kan påvirkes af menneskelig aktivitet, så vi kan ikke afvise, at de indsamlede sensordata kan udgøre en personoplysning. Ved brug af det andet kriterie ser vi, at der findes situationer, hvor der kun er enkeltpersoner til stede i klasselokaler. Det vil blandt andet være udenfor undervisning, når rengøringspersonalet passer sit arbejde. Dette kan bruges til at danne et overblik over, hvor lang tid rengøringspersonale bruger i hvert lokale, samt at se hvor de er for et givet tidspunkt. Dermed udgør de indsamlede sensordata en personoplysning.

Et andet eksempel på anvendelse af det andet kriterie i forbindelse med støjmålinger i klasselokaler er, at forskellige lærere underviser forskellige klasser på forskellige tidspunkter. Ved at sammenholde støjmålinger indsamlet i klasselokalerne gennem længere tid og sammenholde disse med skemaerne for både skoleklasser og lærere, er det muligt at forbinde støj i klasserne med specifikke lærere, hvilket kan tyde på, at læreren har svært ved at kontrollere klassen. Det vil sandsynligvis også være muligt at kontrollere for svære klasser (skoleklasser, hvor støjniveauet er højt uafhængigt af læreren) og lokaler med høj genklang (lokaler med et højt støjniveau uanset klasser og lærere). Dette ville give en måling af en undervisers evne til at kontrollerer klassen, hvilket udgør en personoplysning.

4 | Har vi hjemmel til at behandle personoplysninger?

Før vi kan indsamle og behandle personoplysninger, må vi have det nødvendige lovgrundlag; en såkaldt hjemmel. GDPR lister i alt seks mulige hjemler til indsamling af personoplysninger. Eftersom vi diskuterer, hvordan kommunerne kan bruge Smart City til at styrke de kommunale serviceydelser, giver det mest mening at fokusere på hjemlen "*En opgave i samfundets interesse eller offentlig myndighedsudøvelse*" (*SOIM*). Det giver, som navnet siger, hjemmel til at indsamle og behandle

personoplysninger, når disse er nødvendige for at kunne udføre en opgave i samfundets interesse eller offentlig myndighedsudøvelse. Den kræver, at der er en underliggende lov, der begrunder hjemmelen, ved enten at give en organisation pligt at udføre en opgave eller autoritet (GDPR Art. 6, Par. 1 & 3). Denne kan videreføres til en tredjepart, hvis tredjeparten har aftalt med en offentlig instans at udføre opgaven for dem, dvs. hvis tredjeparten er databehandler på opgaven, og der er udarbejdet den nødvendige databehandleraftale.

For at kunne anvende SOIM hjemlen til at behandle personoplysninger for at fuldføre en opgave, skal vi altså først identificere de love, der giver en kommune ansvar for at løfte den konkrete opgaven.

4.1. Opfylder Climify's formål en opgave beskrevet i lov?

Som sagt er formålet med Climify primært at sikre godt indeklima i skolerne og sekundært at give elever og undervisere et indblik i deres eget indeklima. Vi skal altså identificere en lov, der beskriver denne opgave.

En kort gennemgang af lovgivningen giver os to love der tilsammen matcher disse kriterier: Undervisningsmiljøloven og Bygningsreglementet.

Undervisningsmiljøloven kapitel 1 og 4, siger, at undervisningsinstitutioner skal:

- Sikre et godt, sundt og trygt undervisningsmiljø for elever og studenter.
- Udgive en undervisningsmiljøvurdering der:
    - Beskriver fysisk, psykisk og æstetisk undervisningsmiljø.
    - Er tilgængelig på skolen for elever, studenter og andre interessenter.
    - Opdateres ved ændring af undervisningsmiljø, dog mindst hvert tredje år.

For at konkretisere disse krav, må vi identificere en offentlig standard for, hvad der definerer et sundt og trygt undervisningsmiljø, hvilket beskrives i Bygningsreglementet kapitel 22 og 19, der har følgende regler:

- Der er en øvre grænse for, hvor meget CO2 der må være i et undervisningslokale.
- Termisk indeklima skal være komfortabelt i lokaler, hvor personer opholder sig i lang tid.

Vi har dermed juridisk belæg for at indsamle og overvåge CO2, fugt og temperatur. Vi kan også argumentere for at støj niveau indgår i fysisk undervisningsmiljø, da et studium udgivet af Branche Fællesskab for Arbejdsmiljø viser, at det er sværere for elever at koncentrere sig, når der er meget støj i lokalet.

5 | Bliver data behandlet i overensstemmelse med formålet?

Et kerneprincip i GDPR er, at når data bliver behandlet for at opfylde et formål, så skal der kun bruges den mængde data, som er krævet for at opfylde formålet; dette kaldes ofte dataminimering. Hvis vi f.eks. har som formål at sende en SMS med en fødselsdagshilsen, så er der kun behov for navn, fødselsdato og telefonnummer. Det ville være overdrevet at tilgå personens fulde CPR-nummer for dette formål.

Vi skal dermed afklare, hvilke hjemlede formål vi har for at behandle data, samt sikre at de data der behandles udgør den mindst mulige mængde af data, der er nødvendig for at opnå formålet. Hvis

det er muligt at få adgang til flere data end nødvendigt, er det nødvendigt at finde måder at håndtere dette problem. Vi kan begrænse mængden af data, der er tilgængelig, f.eks. ved at slette data, der ikke er nødvendige for den specifikke opgave, eller vi kan bruge tekniker til at transformere data, så de ikke længere udgør personoplysninger, f.eks. gennem anonymisering, randomisering, generalisering, eller andre metoder. En anden mulighed er at begrænse adgang til formålet, så der kun er adgang til data for specifikke personer, eller at data kun kan tilgås i bestemte situationer. Er formålet generelt, kan det være at forskellige mængder data ville være passende i forskellige kontekster. Her kan det give mening at splitte formålet op i et underformål for hver kontekst. Dermed skal der ikke være avancerede mekanismer for at håndtere flere kontekster i generelle formål.

5.1. Hvordan kan Climify afgrænse behandling af data til indsamlings formål?

Vi vurderer her om Climify indsamler data, der passer til deres formål. Det kan være nødvendigt at transformere eller begrænse adgang til data eller at splitte formål op til mere specifikke underformål. Som tidligere diskuteret har Climify to formål. Der skal sikres et sundt undervisningsmiljø i skolerne, og en undervisningsmiljøvurdering skal gøres tilgængelig for interessenter. Vi kalder dem henholdsvis *IndeklimaVedligehold* og *Undervisningsmiljøvurdering*.

IndeklimaVedligehold er relativt lige til. Ikke alle har behov for adgang til indeklimadata. Som diskuteret i sektion 2 ville det give mulighed for misbrug, hvis f.eks. skoleinspektøren frit kan læse indeklimadata. Derfor giver det mening at begrænse adgang til indeklimadata til personer, der er ansvarlige for at opretholde indeklima på skolerne. Dermed kan de lave relativt dybe analyser, og finde nye måder at forbedre og vedligeholde indeklima.

Undervisningsmiljøvurdering er mere komplekst. Climify skal offentliggøre en indeklimavurdering til elever, studenter og andre interessenter. Hvem disse interessenter er, kan fortolkes bredt; det kunne principielt være hele befolkningen. Her giver det god mening at offentliggøre aggregerede data for hele skolen, således at personer udenfor skolen kan få et hurtigt overblik over, hvilke skoler har et bedre indeklima. Det kunne også fortolkes mere specifikt som personer, der har en tilknytning til skolen. Ansatte, administration, elever og forældre. Hvis disse grupper får adgang til aggregerede data for de enkelte lokaler, kan de se, hvilke lokaler der kræver udredninger. Endelig kunne det være interessant at give personer adgang til deres egne indeklima data; det vil sige indeklimadata optaget i lokaler, mens de var i lokalet. Dette ville være en meget specifik fortolkning af undervisningsmiljøloven, men det er i overensstemmelse med rettigheden vedrørende dataindsigt, der giver personer adgang til deres egne personoplysninger.

Dermed kan vi dele Undervisningsmiljøvurdering formålet op i tre forskellige underformål: *Offentlig*, *Intern* og *Personlig*.

Det er enkelt at afgøre, hvem der opfylder kravene for de fleste af de beskrevne formål. Skolerne ved, hvem der er ansvarlige for indeklima, samt hvem der er ansatte, elever osv. Der er dog en udfordring i at bestemme, hvem der var i rummet på data indsamlingstidspunkt. Vi foreslår tre metoder.

- Personen har en forbindelse til skolen (medarbejder, elev, forældre til elev, etc.), og skolen var åben på det givne tidspunkt.
- Personen havde skemalagt undervisning/arbejde i lokalet på det givne tidspunkt.
- Sensorer i lokalet registrerede personens nærvær på det givne tidspunkt.

Det første forslag rammer bredt. Givet at indeklimadata vurderes at være personhenførbare data, risikerer vi, at personer får adgang til data fra lokaler, de ikke har været, og dermed får adgang til data, de ikke har behov for. Dette betyder, at denne metode ikke kan stå alene, men at der bør introduceres yderligere kontroller for at sikre, at der kun gives adgang til data efter behov.

Det andet forslag risikerer at give adgang til data, når de ikke har været i lokalet, men dette burde være begrænset til isolerede tilfælde, og repræsenterer noget skolerne kan implementere i dag.

Det tredje forslag involverer digital overvågning af mindreåriges fysiske lokationer. Vi har i dag teknologien til at understøtte dette, f.eks. via elevernes mobiltelefoner, hvilket på nogle måder kan sammenlignes med de navneopråb, man benytter i dag. Dette er dog på andre måder langt mere indgribende, fordi den nødvendige tekniske infrastruktur ville tillade kontinuerlig overvågning af elever og måske også lærere; både i timerne og i frikvartererne.

Dermed har vi en plan for, hvordan vi kan begrænse adgang til indsamlet data, så det passer med de formål dataene er blevet indsamlet til at opfylde. Dette er illustreret i tabel 1.

Subjekt	**Formål**	**Udstillet data**
Indeklimaansvarlig	IndeklimaVedligehold	Indeklimadata
Offentligheden	Offentlig Undervisningsmiljøvurdering	Aggregeret data for skole
Alle tilknyttet en skole	Intern Undervisningsmiljøvurdering	Aggregeret data for lokale
Alle	Personlig Undervisningsmiljøvurdering	Indeklimadata optaget når personen var i lokalet

Tabel 1: Plan for hvem der må behandle hvilket data

6 | Konklusion

Vi har nu dækket nogle af problemstillingerne, der vil blive mødt ved udviklingen af et Smart City projekt. Med introduktionen af Climify projektet har vi illustreret, hvordan en kommune kan afgøre, om indsamlet data udgør personoplysninger. Dette kræver i givet fald en hjemmel under GDPR, hvorfor vi diskuterede, hvordan hjemmel bliver givet, når samfundet giver kommunerne en opgave ved lov. Dette betyder ikke, at kommunerne kan behandle alle typer af data, men skal vise, at behandling af personoplysning bliver gjort i overensstemmelse med de hjemlede formål, som data bliver indsamlet til.

Dette giver et kort indblik i den håndbog, vi arbejder på i SAnD projektet, og som vi håber at kunne offentliggøre i første halvdel af 2021. Vi planlægger, at håndbogen dykker lidt dybere ned i nogle af de emner, vi ikke har kunnet dække i denne artikel. Diskussioner om, hvilke hjemler der passer med Smart City udvikling, hvilke rettigheder registrerede personer har, når deres personoplysninger bliver behandlet med hjemmelen SIOM, samt hvordan kommunerne dokumenterer, at data bliver behandler i overensstemmelse med hjemlede formål.

Håndbogen kommer ikke ind på nogle af de dybere kompleksiteter, der opstår i forbindelse med GDPR, såsom databehandler aftaler og risikovurderinger (DPIA), men er tænkt som et første spadestik i spørgsmålet om, hvorvidt kommunerne har tilladelse til at behandle smart city data, og hvordan de kan komme i gang med at gøre dette.

Vi er ikke juridiske eksperter, men har god forstand for datasikkerhed. Tag dermed vore juridiske vurderinger med et gran salt.

7 | Referencer

Undervisningsministeriet (2017). *Undervisningsmiljøloven*, Retsinformation at https://www.retsinformation.dk/eli/lta/2017/316, [Tilgået 4 december 2020].

Trafik-, Bygge- og Boligstyrelsen (2020). *Bygningsreglementet*, Bygningsreglementet, på https://bygningsreglementet.dk/, [Tilgået 4 december 2020].

Branche Fællesskab Arbejdsmiljø (BFA) (2018). *Støj I Skolen*, Arbejdsmiljøweb, på https://www.arbejdsmiljoweb.dk/media/o2uehuao/stoej-i-skolen_2018_web.pdf, [Tilgået 4 december 2020].

Justitsministeriet (2016). *EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016*, Retsinformation, på https://www.retsinformation.dk/eli/lta/2018/502, [Tilgået 4 december 2020].