Håndbog i Smart City Privacy

Guide til håndtering af persondata i Smart City-projekter

Eirik Oterholm Nielsen
Christian D. Jensen

Udgivet for projektet Sikker og Anvendt Data, støttet af Region Hovedstaden.

Parterne bag Sikker og Anvendt Data projektet SAnD:
Gate 21, Region Hovedstaden, Danmarks Tekniske Universitet (DTU/DTU Compute),
Høje-Taastrup Kommune og Frederiksberg Kommune

Udgivelsen af denne Håndbog i Smart City Privacy er gjort mulig af midler fra Sikker og Anvendt Data projektet SAnD, som er støttet af Region Hovedstaden med medfinansiering af de deltagende parter. Tilrettelæggelse og redaktion er forestået af DTU Compute på vegne af parterne bag projektet.

ISBN nr.: 978-87-643-2004-6
1. udgave. Juni 2021.
Redaktion: Eirik Oterholm Nielsen, Christian D. Jensen, Hanne Kokkegård og Sine Ingemann
Billeder: Colourbox
Grafisk design og opsætning: Bjarne Erick, freelance grafisk designer
Tryk: Vester Kopi

Forord

Brugen af IoT udvikler sig lige nu med en gevaldig fart. Teknologien betyder, at det er blevet meget billigt at indsamle data fra sensorer i bybilledet og lokalt i bygninger og installationer. Frederiksberg Kommune trækker på IoT-teknologi til at udskrive parkeringsafgifter baseret på scanning af bilers nummerplader og koblet med tidspunkt og GPS. I Vallensbæk arbejder kommunen på at regulere trafiklys ved hjælp af GPS-data. Fjernvarmeselskaber styrer fremløbstemperaturen i rørene ved hjælp af vejrdata indsamlet lokalt i området. Og sensordata kan vise, hvor godt bygninger er isolerede, hvis varmeforbruget altid stiger, når vinden kommer fra en bestemt retning.

I dag har kommuner og offentlige og private selskaber dog ofte en berøringsangst over for at indsamle og bruge data af frygt for, at data kan blive anvendt forkert, ligesom de er i tvivl om reglerne for brug af persondata, GDPR. Det bremser udrulningen af Smart City-teknologier og services, der også er nødvendige i den grønne omstilling.

I denne håndbog giver vi en kort gennemgang af flere GDPR-principper og viser, hvordan de kan påvirke et Smart City-projekt.

Håndbogen rummer også en tjekliste, som kommuner, virksomheder, forsyningsselskaber og andre kan udfylde for at få overblik over brugen af persondata. Tjeklisten kan samtidig bruges som et værktøj i forbindelse med behandling af projektplaner.

Det er vigtigt at understrege, at vi er eksperter i IT-sikkerhed, men vi er ikke jurister. Så vi anbefaler kraftigt, at I inddrager jeres organisations jurister og får tjekket, at I har fået klarlagt det hele, før I går i gang med dataindsamling. På nuværende tidspunkt er der også kun faldet dom i relativt få sager om persondata, så retspraksis er endnu ikke på plads på området.

Vi håber dog, at håndbogen giver anledning til en mere kvalificeret diskussion om brug af data i Smart City-projekter. Vi håber også, at den vil give jer det fornødne overblik og være med til at bane vej for mere datadreven nytænkning i smarte byer.

God læsning!

Christian D. Jensen
Lektor, sektionsleder for Cyber Security på DTU Compute
Juni 2021

Sammenfatning – håndtering af persondata i Smart City-projekter

Persondata: Er der opsamlet data, som identificerer personer?

- Information er personoplysning, hvis den kan henføres til en fysisk person, eller hvis det kombineret med anden information identificerer en fysisk person, også selv om de projektansvarlige ikke kan gøre det.
- Overvej beregningsmetoden i datahåndteringen og hvordan data bliver fremlagt for at undgå personoplysninger.
- Er der ikke personoplysninger, kan projektet anvende egne opsamlede data uden begrænsning.

Personoplysninger kan være:

- Abstrakt information som et navn eller et pseudonym
- Konkret information som lokation, tilhørsforhold til en adresse eller til en organisation
- Oplysninger vedrørende opførsel som en bankoverførelse eller gæstebog
- Fysisk information som højde, alder eller sygdomshistorie

Hjemmel: Har vi lov til at indsamle data?

GDPR nævner seks former for hjemmel til at indsamle og behandle data:

- Informeret samtykke
- En kontrakt med den registrerede
- Den dataansvarliges retlige forpligtelser
- Den registreredes eller en anden fysisk persons vitale interesser
- En opgave i samfundets interesse eller offentlig myndighedsudøvelse (SIOM)
- En legitim interesse, som ikke overgås af den registreredes interesser eller rettigheder

Rettigheder: De registreredes ret til egne data

GDPR-reglerne sikrer den registrerede flere forskellige rettigheder i forhold til egne data.
Rettighederne afhænger af, hvilket formål data bliver indsamlet under:

- Ret til indsigt
- Ret til berigtigelse
- Ret til sletning (gælder ikke SIOM)
- Ret til begrænsning af behandling
- Ret til dataportabilitet
- Ret til indsigelse
- Ret til ikke at være genstand for en automatisk afgørelse

Formål: Begræns mængden af formålsdatabehandling til mindst mulig

Et kerneprincip i GDPR er, at vi kun skal opsamle de data, vi har brug for til at løse opgaven.
Begræns adgang til data og formål, så kun bestemte personer har adgang til den mængde data, som de har brug for til at løse opgaven.
Opsplit projektet i flere formål, så forskellige mængder data kan indsamles i forskellige kontekster.

Sikkerhedsmodellen: Sådan får man styr på privacy

Skab overblik over dataindsamlingen i projektet i forhold til formål, dataabstraktion, intern og ekstern adgang til data.

Indhold


CAM-10

Introduktion

IoT er i hastig udvikling. Teknologien betyder, at det er blevet billigt at indsamle data fra sensorer i bybilledet. Batterier holder f.eks. længere, så de ikke skal udskiftes så ofte. Det er samtidig blevet mere effektivt at sende data trådløst over netværk, som LoRaWAN. Det giver nogle rigtig spændende muligheder for at udvikle Smart City-teknologier.

Uanset om det gælder trafikstyring, spildevandsmåling eller indeklima i skoler, så er der stort potentiale i at sætte sensorer op og finde ud af, hvordan byen og services kan forbedres.

Der er dog tilsvarende en stor risiko for, at data kan blive misbrugt. Kameraet, der tæller biler, kan bruges til at overvåge opførsel på gaden. Og sensoren, der tjekker indeklimaet på et kontor, kan bruges til at bekræfte, hvorvidt kontorets ejer er tilstede.

GDPR-reglerne skal forhindre misbrug af persondata, og når reglerne bliver overtrådt, kan der blive udstedt store bøder.

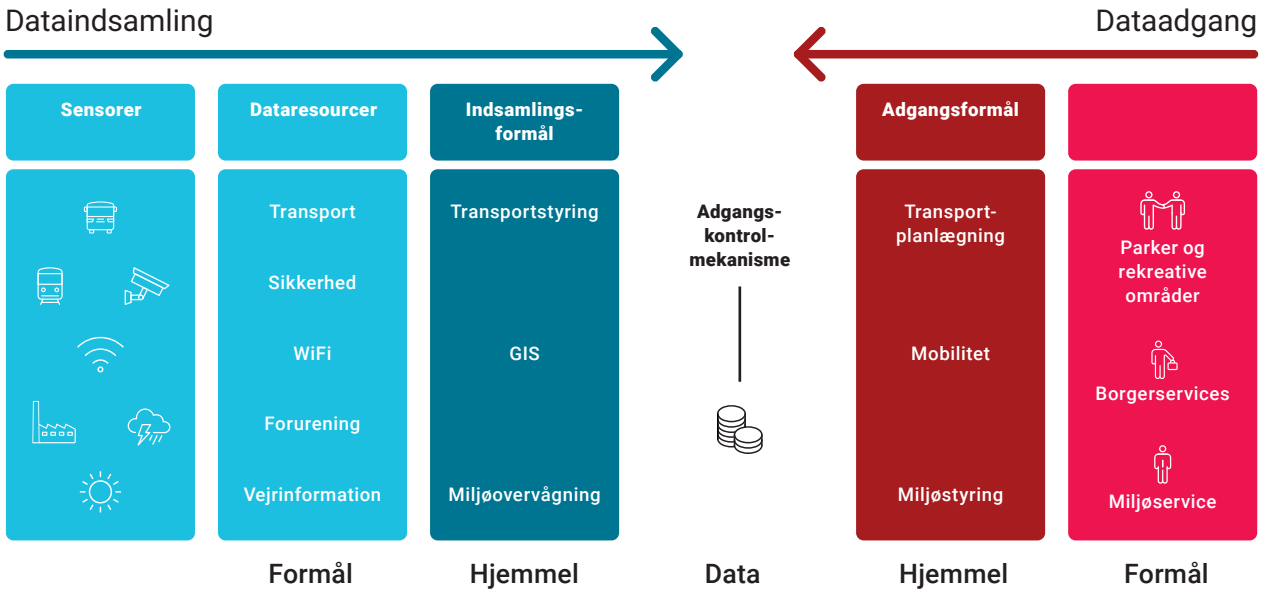
De dataansvarlige skal kunne afgøre, hvorvidt de data, de indsamler, er persondata. De skal også kunne klargøre, hvorvidt de har hjemmel til at indsamle disse data. Afhængig af hvilken hjemmel persondata bliver indsamlet under, så har de registrerede personer forskellige rettigheder, hvilket der også skal tages hensyn til.

Når en offentlig myndighed indsamler personoplysning, er det derfor essentielt at vide, hvilket formål data skal bruges til, og med hvilken hjemmel data bliver indsamlet. Desuden skal det være klart, hvordan data bliver anonymiseret eller beriget med nye oplysninger, så borgeren og andre kan sikre sig, at reglerne bliver overholdt (compliance).

I denne håndbog vil vi med udgangspunkt i et konkret Smart City-projekt vise, hvordan de projektansvarlige får overblik over reglerne for privatliv (privacy). Vi gennemgår overvejelser og regler trin for trin og sammenholder med casen.

Vi fokuserer med GDPR-rettighederne primært på, hvordan Smart City-udviklere kan opfylde registreredes rettigheder til dataindsigt. Vi viser teknikker til, hvordan vi dokumenterer, at indsamlet data bliver anvendt til formål, som vi har lov til, at registrerede skal kunne få adgang til deres data, samt at de skal kunne se, hvordan deres data bliver sikret, og hvorfor deres data bliver brugt. Fig. 1 viser hvordan persondata er beskyttet med håndhævelse af GDPR, at indsamling af data skal ske inden for en hjemmel, og at der skal være et klart formål med indsamlingen af data.

Fig. 1 **Beskyttelse af privatlivets fred med håndhævelse af GDPR**



Casestudie: Smart City-projektet Climify

Igennem denne håndbog bruger vi Climify som eksempel på et Smart City-projekt, der indsamler data fra forskellige sensorer.

Climify er et projekt, der bliver udviklet på DTU i samarbejde med en række kommuner, hvor de kommunale folkeskoler bruger hjemmesiden Climify.com og en tilknyttet app til at indsamle og præsentere en række former af indeklimadata:

- Lydniveau
- Temperatur
- CO_2
- Luftfugtighed

Disse indeklimadata bliver indsamlet af sensorer fra forskellige producenter, blandt andre Elsys, NorthQ og IC-Meter. Sensorerne er sat op i forskellige lokaler og konfigureret til løbende at sende indeklimadata til Climify-serveren, så man både får registreret klokkeslæt for målingerne og lokalet. Indeklimadata kan derefter vises på kort over skolerne og i grafer, og data kan også trækkes ud af serveren. Indeklima på kort og graf er illustreret henholdsvis i figur 2 og 3 på side 10.

Det primære formål med hjemmesiden er at sikre et godt indeklima på de skoler, der bruger løsningen. Driftsfolk med ansvar for indeklimaet kan let aflæse, hvordan det står til med indeklimaet i skolens lokaler her og nu, og f.eks. før og efter tiltag bliver sat i gang. Tiltagene kan være i forhold til netop indeklimaet, men data kan også være med til at forbedre skolernes energiforbrug, f.eks. forbedret isolering af lokaler eller nye ventilationssystemer.

Tiltag kan også være uddannelse af elever og lærere i, hvordan de bedst selv regulerer indeklimaet gennem udluftning. Her vil elever og lærere kunne få adgang til Climify via en app, hvor de kan se, hvordan deres handlinger påvirker indeklimaet. Det vil samtidig give elever og lærere mulighed for at få bekræftet, om de har det undervisnings- og arbejdsmiljø, som de er berettiget til, blandt andet igennem undervisningsmiljøloven og arbejdsmiljøloven.

Baseret på vores case er det klart, at data indsamlet i Smart City-projekter kan være værdiskabende.

Det store spørgsmål er, om data er personhenførbar, så man kan identificere en bestemt person ud fra data, for så skal data behandles som personoplysninger og er omfattet af GDPR-reglerne.

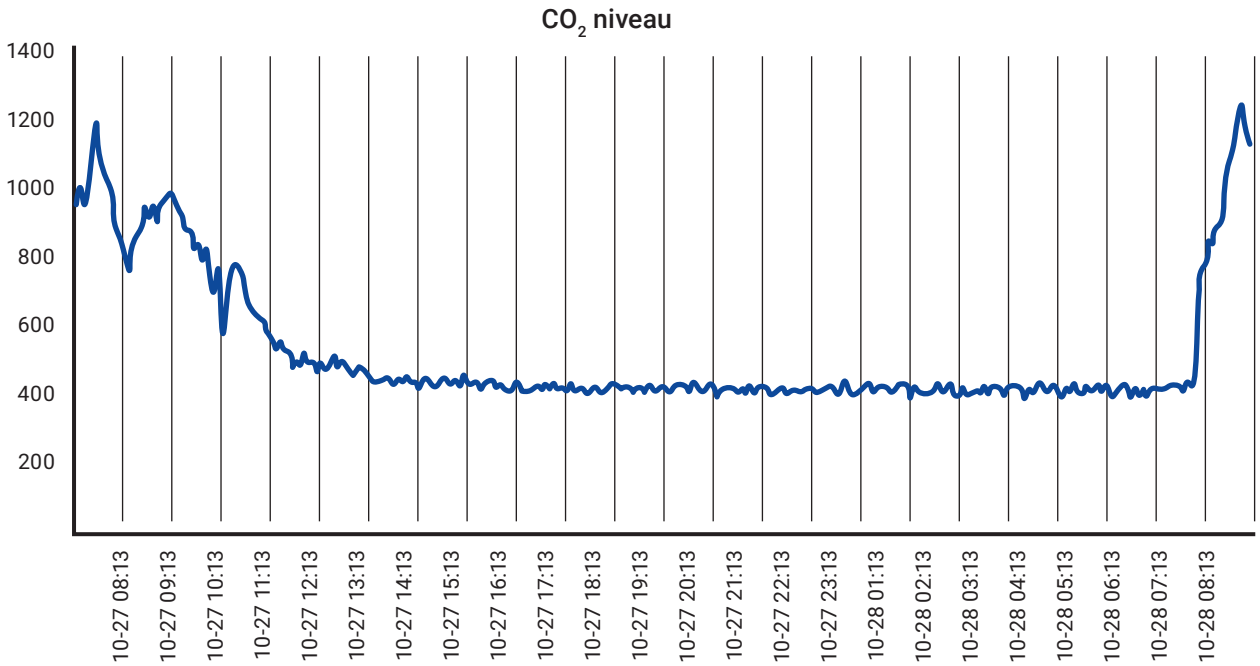
Det afdækker vi på de følgende sider.

Kort om Climify

Climify blev etableret i 2017. I begyndelsen var Climify et værktøj til overvågning af indeklimaet i skoler. Målsætningen var at minimere CO_2-aftrykket og øge elevernes velvære og koncentrationsevne. I løbet af de første år udviklede platformen og projektet sig fra at være en lille og begrænset platform, Skoleklima, til at blive et moderne visuelt værktøj. Climify arbejder i dag med indeklima-overvågning i mange forskellige typer bygninger herunder kontorbygninger, campus-områder, idrætshaller og hospitaler.

Fig. 2 **Gulvplan for skole, hvor indeklima-status i lokaler er illustreret med farve, og man kan få mere specifik indeklimadata for enkelte lokaler.**

Fig. 3 **Indeklimadata for specifikt lokale**



Persondata: Er der opsamlet data, som identificerer personer?

Datatilsynet siger, at information er personoplysning, hvis den kan henføres til en fysisk person. Det er også personoplysning, hvis det kan kombineres med anden information, og dermed henføres til en fysisk person. Desuden er det ifølge Datatilsynet personoplysning, hvis bare en enkelt person kan identificere en bestemt person ud fra data, også selv om vi som Smart City-udviklere ikke selv kan gøre det.

En identificerbar person er ifølge GDPR-artikel 4 [1] en person, der kan direkte eller indirekte identificeres via navn, ID-nummer, lokation, online-pseudonym eller beskrivelser som fysisk, fysiologisk, genetisk, mentalt, økonomisk, kulturelt eller social identitet. Det er altså personoplysninger, når vi ud fra data kan se hvilken person, der er tale om. Det betyder, at rigtig meget data hører til under kategorien 'personoplysninger'.

Bemærk også, at hvis vi i Smart City-projekter finder ud af, at data ikke under nogen omstændigheder vil kunne kobles til bestemte personer, så kan vi frit indsamle og anvende data, så længe vi selv ejer data.

Det første skridt er at afgøre, hvorvidt data beskriver personer. Det gør den kun, hvis data bliver påvirket af mennesker. Et udendørs-termometer vil i de fleste situationer ikke have noget med en person at gøre, for temperaturen ændrer sig ikke målbart, selvom der er en person i nærheden.

Temperaturen i et lokale kan derimod variere på grund af menneskelig aktivitet. Det kan være et lille gymnastikhold, der opvarmer et underdimensioneret lokale, eller en medarbejder, der fryser og skruer termostaten op.

Det næste skridt er at vurdere, hvorvidt denne menneskelige aktivitet reelt kan forbindes til en enkelt person. Hvis det kun er én person, der kan påvirke hvert enkelt datapunkt, så er det selvfølgelig klart, at de indsamlede data netop beskriver denne person. Det kan være personens aktivitet, tilstedeværelse eller eventuelle andre faktorer. Dermed bliver det personoplysning.

Det sidste skridt er at afgøre, om en enkelt person vil kunne påvirke datasættet så meget, at det er målbart forskelligt, når data bliver indsamlet for denne ene person og ikke en anden person. Se faktaboks om robust statistik på side 14.

Den samme information kan eksistere i forskellige former, med forskellig specificitet. Dette kunne være information om, at en person har været et sted på et bestemt tidspunkt. F.eks. at person x var i lokale 1.12B klokken 13:45, og person x var i bygning 12 mellem klokken 13 og 14. Vi kalder disse forskellige former af samme information for dataabstraktioner.

For at illustrere hvordan forskellige dataabstraktioner kan bruges til at anonymisere data, der offentliggøres, betragter vi følgende scenarie:

Skolerne i en kommune offentliggør CO_2 målinger fra alle lokaler hver halve time. En skoles to gymnastiksale bruges om aftenen af forskellige idrætsforeninger i kommunen. For at vise kommunens borgere, at gymnastiksalene ikke opvarmes forgæves, ønsker kommunen at udstille udnyttelsesgraden af gymnastiksalene på en måde, der ikke hænger de individuelle idrætsforeninger ud. Alle idrætsforeninger har uger, hvor der ikke trænes, disse meddeles kommunen, som ikke opvarmer gymnastiksalene på disse dage, og de tæller derfor heller ikke med i udnyttelsesgraden.

Idrætsforeningernes program kendes, så hvis kommunen udstiller udnyttelsesgraden af de enkelte gymnastiksale, vil idrætsforeninger, der ikke udnytter en given gymnastiksal direkte, kunne identificeres. For at anonymisere idrætsforeningernes udnyttelse af skolens gymnastiksale, kan skolen definere dataabstraktioner af enten tid eller sted. Et sådant eksempel er vist i skema 1, side 12.

Skema 1 **Anonymisering gennem dataabstraktioner**

	Gymnastiksal 1	**Skole**
Mandag aften	Idrætsforening, der ikke udnytter gymnastiksalen, kan direkte identificeres.	Idrætsforening, der ikke udnytter gymnastiksalen, kan identificeres ved at sammenholde med CO_2 målingerne, hvilket afslører om der er aktivitet i lokalet.
Ugenummer	Idrætsforening, der ikke udnytter gymnastiksalen, kan identificeres ved at sammenholde med CO_2 målingerne, når der kun er en enkelt ugedag, hvor CO_2 målingerne indikerer, at der ikke er aktivitet i gymnastiksalen.	Idrætsforening, der ikke udnytter gymnastiksalen, kan kun identificeres, hvis udnyttelsesgraden svarer til, at der kun er én idrætsforening, der er udeblevet, og der kun er et enkelt tidspunkt på ugen, hvor CO_2 målingerne indikerer, at der ikke er aktivitet i gymnastiksalen.

Der er mange måder at introducere dataabstraktioner for at hjælpe med at anonymisere eller pseudonymisere data, men de mest oplagte relaterer til tid og sted. Ved at vælge at rapportere måledata med reduceret opløsning, udstiller man resultatet af flere målinger i den samme dataværdi. Opløsningen af målinger i tid og sted kan reduceres ved at betragte følgende hierarkier:

Tid: sekund $\subseteq$ minut $\subseteq$ time $\subseteq$ dag $\subseteq$ uge $\subseteq$ måned $\subseteq$ år

Sted: lokale $\subseteq$ etage $\subseteq$ bygning $\subseteq$ skole $\subseteq$ kommune $\subseteq$ land

Som det ses af ovenstående eksempel, er det vigtigt at vælge en opløsning, der sikrer, at de enkelte udstillede datapunkter ikke kan føres tilbage til en enkelt person, når man danner fællesmængden mellem alle udstillede data.

Eksempler på personoplysninger:

- Abstrakt information som et navn eller et pseudonym.
- Konkret information som tilhørsforhold til en organisation eller en adresse.
- Oplysninger vedrørende opførsel som en bankoverførelse eller gæstebog.
- Fysisk information som højde, alder eller sygdomshistorie.

Overstående er ikke en komplet liste over mulige personoplysninger. Den viser blot, at begrebet 'personoplysning' dækker bredt.

Vi skal afgøre, om der er tale om personoplysninger, hver eneste gang vi ønsker at indsamle en ny form for data. Og vi skal huske, at data kan blive personoplysning, hvis der senere opstår nye former for oplysninger, der henfører indsamlet data til én person. Vi kan afgøre det ved at stille spørgsmål, om hvorvidt de nye data rent faktisk kan identificere en fysisk person, og om data kombineret med andre data kan identificere en fysisk person.

Overvågning af individer

Data indsamlet i lokaler, hvor der kun er enkeltpersoner, vil naturligvis være data, der beskriver personen, hvis data altså bliver påvirket af personen. CO_2-niveauet i klasselokaler er netop et eksempel på det.

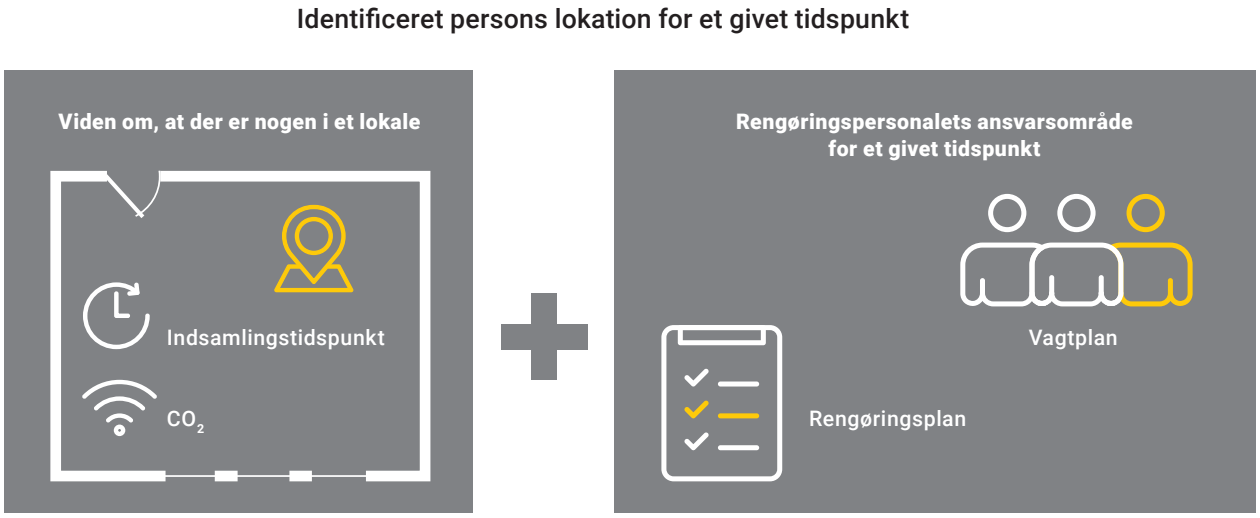
Lad os tage udgangspunkt i, at der er opsat CO_2-sensorer i lokaler på en skole, og at disse sensorer er sensitive nok til at registrere CO_2-ændring i luften, når bare en enkelt person opholder sig i lokaler beregnet til undervisning.

Ved at forbinde CO_2, indsamlingstidspunkt og lokale kan vi danne os et billede af hvilke lokaler, der opholder sig personer i. Hvis vi har kendskab til arbejdsprocesserne for rengøringspersonalet og ved, at de går rundt på skolen alene, så er det nemt efter skoletid at se, hvor rengøringspersonalet er, og hvor lang tid de bruger i hvert lokale.

Vi kan måske endda forbinde denne information med en rengøringsplan og en vagtplan og dermed vide, hvem der er i gang med at vaske hvor, og hvorvidt personalet overholder rengøringsplanen. Vi kan altså overvåge enkeltpersoner, der færdes på skolen.

Eksemplet illustrerer dermed, at CO_2-niveauet er personinformation, når sensordata bliver indsamlet med tilstrækkelig høj præcision. Dataforbindelserne er illustreret i figur 4.

Fig. 4 **Hvordan CO_2-målinger kan kombineres med andre oplysninger og dermed overvåge rengøringspersonale**



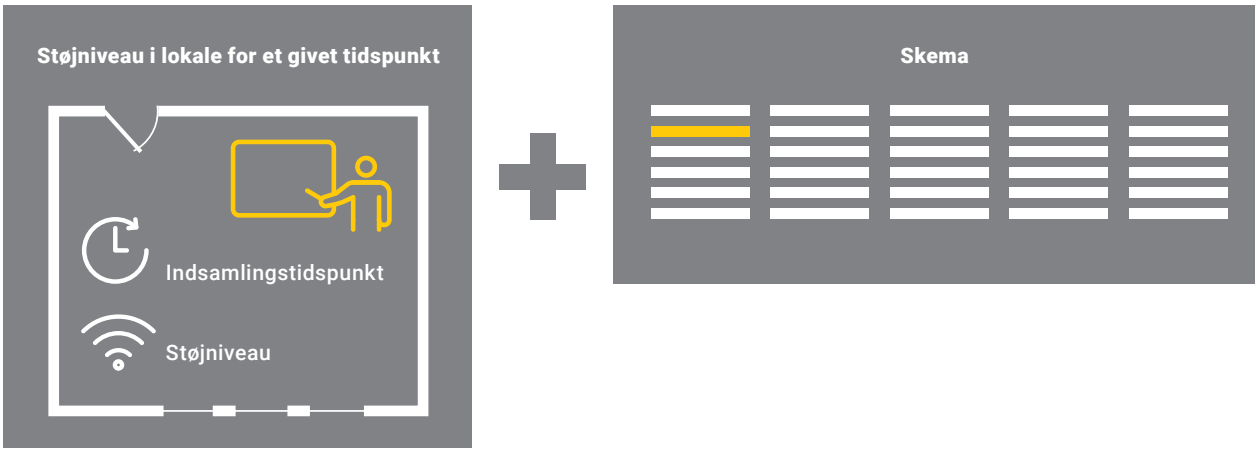
Når én person skiller sig ud i en gruppe

Vi kan altså konkludere, at indsamling af indeklimadata i lokaler, hvor der kun er enkeltpersoner, er indsamling af personoplysninger. Den problemstilling kan muligvis undgås ved kun at indsamle indeklimadata i forbindelse med undervisning. Men samtidig kan indeklimadata indsamlet under undervisning også være personoplysning, hvis vi kan se forskel i indeklimadata baseret på identificerbare personers tilstedeværelse i lokalet.

En klassisk måde, til at afgøre hvor godt styr en lærer har på sine klasser, er, at se på, hvor meget larm der er i lokalet. Hvis vi kombinerer støjniveau, lokale og indsamlingstidspunkt med skolens skema, så er det muligt at se, hvor meget støj, der er i hver klasse, når en bestemt lærer underviser eleverne. Dette er illustreret i figur 5.

Skolen kunne så opgøre forskelle imellem klasser og lokaler og få indblik i lærerens evne til at styre klasserne. Tilsvarende kunne man finde ud af, hvilke undervisere der er gode til at styre indeklimaet i lokalerne, hvis man brugte andre indeklimadata indsamlet i Climify.

Fig. 5 **Hvordan støjniveau-målinger kan kombineres med andre oplysninger og dermed overvåge undervisere.**



Scenarierne viser tydeligt, at selv neutrale data kan bruges til at overvåge individer, også selv om den indsamlede data vedrører en gruppe. Det gælder så længe, der er individer i gruppen, der skiller sig ud, og at de kan findes ud fra indsamlet data.

Det betyder dog ikke, at Smart City-projekter ikke kan gennemføres, hvis man får persondata. Det betyder blot, at projektet skal have hjemmel til at opsamle, lagre og behandle disse data for ikke at overtræde persondataforordningen, GDPR.

Robust statistik

Når man i planlægningsfasen skal beslutte sig for indsamling af data, vil det være oplagt at overveje, hvilke data man ønsker at trække ud af materialet og måske især, hvordan data offentliggøres.

Hvis resultatet af en måling påvirkes af en enkelt persons tilstedeværelse, er der risiko for, at data på et eller andet tidspunkt må betragtes som persondata, fordi der allerede kan eksistere eller senere opstå andre datasæt, der i kombination med de offentliggjorte målinger tillader personen at blive identificeret. Det er derfor vigtigt at overveje hvordan data udstilles, og hvilke egenskaber ved data der offentliggøres. Hvis en kommune f.eks. offentliggør en oversigt over den gennemsnitlige årsindtægt for kommunens borgere i forskellige områder, så vil en enkelt borger med en meget stor indtægt trække gennemsnittet i dette område markant op, hvilket betyder, at det bliver relativt nemmere at finde borgerens bopæl, når man ikke skal søge i hele kommunen men kun i dette område. Sammen med andre offentliggjorte data, om eller fra dette område, kan det således være muligt at identificere den meget velhavende borgers bopæl. Eksemplet illustrerer det problem at nogle statistiske metoder til at sammenfatte data, som f.eks. udregning af gennemsnit, kan påvirkes vilkårligt af et enkelt datapunkt. I mange sammenhænge betragtes sådanne ekstreme datapunkter som outliers, der opstår på grund af målefejl. Der er derfor udviklet statistiske metoder, der er robuste over for tilstedeværelsen af outliers, såkaldt robust statistik. Disse metoder gør det altså muligt at beskrive eller sammenfatte data, uden at outliers slår igennem, hvilket betyder, at enkeltpersoner bliver sværere at identificere i de offentliggjorte data. Kommunen i det ovenstående eksempel kunne sammenfatte data ved at offentliggøre medianen – dvs. den værdi, hvor der er lige mange indtægter, der ligger over og under – i stedet for gennemsnittet, hvorved alle kommunens borgere kan danne sig et billede af den relative velstand i de forskellige områder i kommunen, uden at området hvor den meget velhavende borger har bopæl, kan aflæses i tallene.

Ved at benytte robuste statistiske metoder opnår man ofte en bedre beskyttelse af borgernes persondata, hvilket gør det nemmere at offentliggøre data eller bruge dem i forskellige sammenhænge, fordi outliers der kan være med til at identificere enkeltpersoner ikke fremtræder så tydeligt i data.


JUSTICE

Hjemmel: Har vi lov til at indsamle data?

Når vi allerede har konstateret, at data indsamlet på Climify eller andre steder kan være personhenførbare, har vi så alligevel ret til at indsamle og bruge dem?

GDPR nævner seks former for hjemmel til at indsamle og behandle data:

- Informeret samtykke
- En kontrakt med den registrerede
- Den dataansvarliges retlige forpligtelser
- Den registreredes eller en anden fysisk persons vitale interesser
- En opgave i samfundets interesse eller offentlig myndighedsudøvelse (SIOM)
- En legitim interesse, som ikke overgås af den registreredes interesser eller rettigheder

Informeret samtykke og kontrakt kræver kontakt med enkeltperson, så de to former er svære at bruge i en Smart City-kontekst, hvor man normalt ikke har personlig kontakt.

Retslig forpligtelse er meget specifik. Den giver udelukkende hjemmel til, at dataansvarlige udfører deres retslige forpligtelser. Det gælder blandt andre banker, når de skal forhindre hvidvask af sorte penge. Her og nu hjælper retslig forpligtelse os ikke med at få Smart City-projekter op at køre, men bestemmelsen kan potentielt give os ekstra ansvarsområder på sigt.

Vitale interesser kan bruges ved Smart City-dataindsamling, men kun i de situationer, hvor det er meget klart, at det er i enkeltpersoners interesse, som ved at kunne redde liv – f.eks. ved røverier eller brand.

Vital interesse må derimod ikke bruges som hjemmel til at behandle personoplysninger af offentlige myndigheder.

Det efterlader os så med hjemmelen: 'En opgave i samfundets interesse eller offentlig myndighedsudøvelse" – herefter omtalt som 'SIOM'.

SIOM tillader offentlige myndigheder, eller virksomheder, der udfører opgaver for en offentlig myndighed, at indsamle og behandle personhenførbare data for at udføre en opgave beskrevet ved lov.

I håndbogens casestudie Climify er der tale om en virksomhed, der udfører en opgave på vegne af danske skoler. Hvis skolerne har ansvar for at sikre et godt indeklima og skal kunne dokumentere med målinger, hvordan det står til, så kan Climify godt påtage sig denne opgave.

Vi tager et kig på dansk lovning på området for at klarlægge hjemmelen:

Ifølge Undervisningsmiljøloven [4] har undervisningsinstitutioner en række ansvar.

Undervisningsinstitutioner skal:

- Sikre et godt, sundt og trygt undervisningsmiljø for elever og studerende (Kapitel 1).
- Udgive en undervisningsmiljøvurdering (Kapitel 4).
  - Beskriver fysisk, psykisk og æstetisk undervisningsmiljø.
  - Er tilgængelig på skolen for elever, studerende og andre interessenter.
  - Skal opdateres ved ændring af undervisningsmiljø, dog mindst hvert tredje år.

Der findes også en offentlig standard for, hvad et sundt og trygt undervisningsmiljø vil sige. I Bygningsreglementet (2018) [5] står der:

- Der er en øvre grænse for, hvor meget CO_2, der må være i et undervisningslokale beregnet på, hvor mange der er i lokalet, og hvor stort det er. (Kapitel 22)
- Termisk indeklima skal være komfortabelt. (Kapitel 19)

Det vil sige, at vi har et meget konkret juridisk belæg for, at CO_2 indgår i et sundt undervisningsmiljø, samt et fornuftigt belæg for at temperatur og fugt (termisk indeklima) også indgår. Efter vores vurdering kan vi også inkludere føromtalte lydniveau, da studier påpeger, at desto mere støj, der er i rummet, desto sværere bliver det for eleverne at følge med i undervisningen. [1] [3]

Vi har altså hjemmel til at indsamle data om fugt, CO_2, temperatur og støj for at bruge det til at forbedre og varetage indeklimaet på skoler. Deraf følger, at Climify også kan udgive en rapport til interessenter, der har ansvar for indeklimaet på skolen. Det vil sige, at Climify har hjemmel til at udføre de opgaver, som de gør i øjeblikket.


GDPR
L DATA PROTECTION
GULATION

Rettigheder: De registreredes ret til egne data

Når vi indsamler og behandler personhenførbare data, så kan disse data identificere mindst én person, der kaldes den registrerede. GDPR-reglerne sikrer den registrerede flere forskellige rettigheder i forhold til egne data.

Datatilsynet har lavet guiden 'Vejledning om de registreredes rettigheder' [2], der beskriver disse rettigheder, der er forskellige alt efter, hvilken hjemmel data er opsamlet under.

Her gennemgår vi kort rettighederne og undersøger, hvad det specifikt betyder, når en offentlig enhed bruger hjemlen SIOM.

- Ret til indsigt
- Ret til berigtigelse
- Ret til sletning
- Ret til begrænsning af behandling
- Ret til dataportabilitet
- Ret til indsigelse
- Ret til ikke at være genstand for en automatisk afgørelse

Ret til indsigt betyder at den registrerede har ret til at:

- Se hvilke af deres data, der bliver anvendt. Personen har også ret til at se data, så længe det ikke går markant ud over andres rettigheder.
- Se hvilket formål data bliver indsamlet til. Herunder hvilken hjemmel, de bliver indsamlet med.

Konkret betyder reglerne for Climify, at firmaet har pligt til ved forespørgsel at dele indeklimadata med de personer, der var i lokalet, da sensorerne målte data. For det vil ikke anses for at gå betydeligt ud over andres rettigheder, selv om der var flere i lokalet på indsamlingstidspunktet. Climify skal også oplyse om, hvordan de behandler data og formålet for dataopsamlingen.

Ret til berigtigelse betyder, at hvis der bliver behandlet data, der er forkert, så har registrerede ret til at få data rettet (berigtiget).

Der er dog lige det men, at når data bliver behandlet med SIOM som hjemmel, så skal historikken bevares. Man må altså ikke slette de forkerte data, når man berigtiger data. I stedet opretter man en ny case med korrekt data og tilføjer en kommentar, der forklarer situationen og arkiverer den gamle case. Hvis man som databehandler er uenig med registrerede person om, hvorvidt indsamlet data er forkert, så er det ikke et krav, at data skal berigtiges.

Et tænkt eksempel kunne være, at Climify's sensorer var defekte og derfor optog 'dårlige' data. For at have en standardiseret indsamling ville det måske være uhensigtsmæssigt at erstatte den med data suppleret af registrerede. Det kunne dog være fornuftigt at markere data optaget af defekte sensorer som ukorrekt.

Ret til sletning gælder ikke for data, der bliver indsamlet med hjemlen SIOM. Det ville bryde reglen om, at offentlige instanser skal varetage førnævnte historik.

Ret til begrænsning af behandling gælder særligt for SIOM. Det giver en person, hvis information bliver behandlet, ret til at bede om, at data ikke skal behandles yderligeres. Den regel kan komme i brug, hvis:

- Den registrerede bestrider oplysningernes korrekthed.
- Oplysninger behandles ulovligt.
- Oplysningerne ikke længere er nødvendige, men der pågår en retssag, hvor data indgår, inden de slettes.
- Registrerede har gjort indsigelse imod behandlingslegitimitet.

I de tilfælde ville Climify midlertidigt skulle stoppe adgang til de specifikke data, indtil sagen var blevet behandlet.

Ret til dataportabilitet gælder ikke for SIOM. Reglen betyder, at data, der bliver udleveret efter ret til indsigt, skal være nemt maskinlæsbar. Hvad 'nemt' indebærer er industri-specifikt, men kan ofte betyde, at data udleveres i f.eks. JSON- eller XML-format.

Ret til indsigelse gælder særligt ved SIOM. Den betyder, at personer - der får indsamlet og behandlet data - har en kanal til at klage, hvis de mener, at deres data bliver behandlet på en forkert måde. F.eks. at hjemlen, der bliver brugt, ikke er korrekt, eller at det ville være fornuftigt at bruge mindre specifik data.

Ret til ikke at være genstand for en automatisk afgørelse betyder, at registrerede har ret til ikke at blive underlagt betydelige afgørelser, der er alene baseret på automatiske profileringer.

Formål: Begræns mængden af formålsdatabehandling til mindst mulig

Et kerneprincip i GDPR er, at når data bliver behandlet for at opfylde et formål, så skal der kun bruges den mængde data, der er behov for. Hvis formålet eksempelvis er at sende en fødselsdagshilsen med sms, så er der kun brug for navn, fødselsdato og telefonnummer. Her ville det være unødvendigt at indsamle personens fulde CPR-nummer.

Vi begynder med at afklare, hvilken hjemmel vores formål hører ind under. Vi vurderer også, hvilke data vi kan nøjes med at indsamle og behandle. Vi undersøger også, om der vil kunne opstå situationer, hvor vi kan komme til at overskride vores ret til indsamling og behandling af data.

Hvis vi kan forudsige, hvor der kan opstå et problem, så kan vi håndtere disse situationer ved at begrænse datamængden, der er tilgængelig, eller bruge teknikker til at transformere disse data, som f.eks. anonymisering, dataabstraktion eller andet.

En anden tilgang kan være at begrænse adgang til data og formål, så kun bestemte personer har adgang til den mængde data, som de har brug for til at løse opgaven.

Vi kan også vurdere, om det vil kunne forsimple processen at opsplitte formålet i flere formål. Det kunne være tilfældet, hvis formålet er relativt bredt, og forskellige mængder data vil være passende i forskellige sammenhænge.

Her ser vi derfor på, om Climify indsamler data, der passer til deres formål, om det er nødvendigt at transformere data, begrænse adgang til data eller at splitte formålet op i mere specifikke dele.

Climify opfylder to opgaver: Den første er sikring af et godt undervisnings- og arbejdsmiljø; den anden er en indeklimafokuseret undervisningsmiljøvurdering.

De data, der bliver bearbejdet for at udføre disse opgaver, skal dermed være den 'mindste mængde' data, der kræves for at udføre disse opgaver. Climify indhenter som beskrevet tidligere CO_2, Støj, Fugt og Temperatur, registreret i realtid og med lokation på skolerne.

Det betyder dog ikke, at vi trods begrænset mængde indhentet data eller opdeling af data, har lov til at dele indeklimadata på Climify med alle, der går på, arbejder eller er ansvarlige for skolen. For som vi tidligere har vist, kan indeklimadata være personinformation, og derfor skal delingen af data afpasses til behovet.

Skolelederen har ikke behov for at vide, præcis hvilken temperatur det er i et vilkårligt lokale. Dette kunne jo netop bruges til at overvåge rengøringspersonen, som tidligere vist.

I vores Climify-case kan vi nu undersøge, hvordan indsamlet data kan tilpasses Climifys formål for at indsamle og behandle personoplysning.

Til at begynde har vi to formål: Der skal sikres et sundt undervisningsmiljø i skolerne, og en undervisningsmiljøvurdering skal gøres tilgængelig for interessenter. Vi kalder dem henholdsvis Indeklimajustering og Undervisningsmiljøvurdering.

Indeklimajustering er relativt lige til. Hvis vi begrænser adgang til indeklimadata til personer, der er ansvarlige for at opretholde indeklima på skolerne, så har vi reduceret muligheden for misbrug betydeligt. Især hvis vi stiller det kriterie, at indeklimadata skal være optaget på en skole, som den indeklimaansvarlige har ansvar for. Dermed kan de lave relativt dybe analyser og finde nye måder at forbedre og vedligeholde indeklimaet på.

Undervisningsmiljøvurdering er lidt mere kompleks. Som nævnt må Climify ikke dele indeklimadata uden, at der er nødvendigt for at opfylde et specifikt hjemlet formål. Climify skal kunne fremvise en vurdering, som alle interessenter må se. Det kan fortolkes bredt, sådan at offentligheden skal have adgang til den. Her giver det god mening at vise et samlet billede med data for hele skolen, så personer uden for skolen kan få et hurtigt overblik over hvilke skoler, der har et godt indeklima.

Hvis vi derimod fortolker interessenter mere specifikt, som personer der har en tilknytning til skolen, så giver det mening at sende aggregerede data for enkelte lokaler til ansatte, administration, elever og forældre, så de kan se, hvilke lokaler der har et problematisk indeklima, og eventuelt kræve nærmere undersøgelser.

Til sidst kunne det også være relevant at give personer adgang til deres egne indeklimadata. Det vil sige indeklimadata optaget i lokaler, mens de var i rummet.

Det er usikkert, hvorvidt loven vedrørende, hvem der skal have adgang til undervisningsmiljøvurderinger, også kan fortolkes, så den giver adgang til indeklimadata for enkelte lokaler. Her kommer rettigheden vedrørende dataindsigt på spil. Eftersom indeklimadata er blevet indsamlet og behandlet med hjelmen SIOM, så kan vi behandle indeklimadata, hvis vi overholder at give personer adgang til deres egne data.

Dermed kan vi splitte undervisningsmiljøvurderings-formålet op i tre forskellige varianter: offentlig, intern og personlig.

- Offentligheden får en ekstern undervisningsmiljøvurdering, der giver aggregeret data for hele skoler. Eksempel: Uffedal Privatskole havde sidste måned otte timer, hvor indholdet af CO_2 i luften var for højt i undervisningslokaler.
- Elever, ansatte, administration og forældre får intern undervisningsmiljøvurdering, der inkluderer aggregeret data for specifikke lokaler. Eksempel: Lokale 0.03B havde uacceptabelt høj temperatur på tre forskellige dage i uge 32, mens der foregik undervisning i lokalet.
- Personer, der har været i et lokale, får personlig undervisningsmiljøvurdering. Det giver dem tilladelse til at se indeklimadata for lokaler, hvor data blev optaget, mens de var i lokalet.

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 dataindsamlingstidspunktet.

Vi foreslår derfor tre metoder til afklaring:

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

Det første forslag rammer bredt. Givet, at indeklimadata vurderes at være personhenførbare data, får personer adgang til data fra lokaler, de ikke har været i.

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 teknologien til at understøtte dette i dag. Dette er dog ikke noget, som vi vil anbefale, at man dækker sig ind under i dag. Der er markant forskel på indgriben i folks privatliv at føre navneopråb verbalt, som man gør i dag, eller at gøre det samme via BlueTooth på elevernes mobiler.

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

Tabel 1 **Hvornår, hvem får adgang til hvilke data**

Subjekt	Formål	Udstillet Data
Offentligheden	Offentlig undervisningsmiljøvurdering.	Aggregeret data på skoleniveau.
Personale/Elever/Kommune	Intern undervisningsmiljøvurdering.	Aggregeret data på lokaleniveau.
Indeklimaansvarlig og HVAC	Varetagelse og forbedring af indeklima.	Rå data.
Person i lokale	Personlig undervisningsmiljøvurdering.	Indeklimadata optaget, når personen var i lokalet.

Sikkerhedsmodellen: Sådan får man styr på persondata

Nu har vi defineret, hvilke formål forskellige grupper må bruge for at få adgang til indsamlet data. Da vi indsamler og behandler data med hjemlen SIOM, skal vi opfylde rettighederne for dem, hvis data vi indsamler.

Dette inkluderer dataindsigt. Vi har allerede drøftet, hvordan vi delvist opfylder dette ved at give personer adgang til egne data. Nu dækker vi resten af denne rettighed, hvor personen, hvis data bliver indsamlet, skal underrettes om, hvorfor deres data bliver indsamlet. Dette gælder både lovgrundlaget, der ligger for indsamling/behandling, hvordan data bliver beriget eller abstraheret, samt hvordan data bliver beskyttet. Dermed skal følgende tre punkter beskrives:

- Formål: Hvorfor indsamler og bearbejder vi data?
- Dataabstraktioner: Hvordan bliver denne data beriget eller abstraheret, og til hvilke formål bliver den indsamlet?
- Politiker: I hvilken kontekst kan disse formål bruges til at behandle denne data?

Beskrivelsen af de tre punkter skal gøres tilgængelig for borgeren, så borgeren har mulighed for at stille kommunerne ansvarlige for indsamling og behandling af data.

I de følgende undersektioner beskriver vi disse tre punkter nærmere. Under hvert punkt holder vi det op imod Climify og bruger de overvejelser, der er blevet lavet.

Formål: Hvorfor indsamler og bearbejder vi data?
Vi skal specificere, hvilket formål vi bruger til at bearbejde data. Da vi allerede har afgjort, at vi bruger SIOM, skal vi fortælle hvilke love, der giver grundlag for vores dataopsamling. Vi skal samtidig klargøre, om der er specifikke fortolkninger.

Hvis der i stedet var tale om f.eks. informeret samtykke, kunne vi referere til, hvordan samtykke kunne gives. Tilsvarende hvis der var tale om vitale interesser, skulle det forklares, hvorfor den hjemmel var gældende.

Derefter skal vi kort beskrive, hvad vores formål med at indsamle og bruge data er:

- Formål: Hvad er vores formål?
- Hjemmel: Type, SIOM, Retslig forpligtelse, etc.
- Lovgrundlag: Hvilke(n) lov(e) er belæg for samling og benyttelse af data. Supplerende: Er der supplerende information, der giver belæg for samling og benyttelse af data?
- Beskrivelse: Beskriv med daglig tale hvad formålet er.

I de nedenstående skemaer udfylder vi beskrivelserne for Climify og bruger hjemlen diskuteret i forrige afsnit og tabel 1. Vi indsamler og bearbejder indeklimadata, der omfatter lydniveau for at kunne varetage og sikre et godt indeklima. Da personer har ret til at få adgang til egne data under GDPR, kan vi producere en personlig undervisningsmiljøvurdering. Disse er beskrevet i henholdsvis tabel 2 og tabel 3.

Tabel 2 **Formål: Indeklima / Vedligehold**

Formål	Indeklima / Vedligehold
Hjemmel	En opgave i samfundets interesse eller offentlig myndighedsudøvelse.
Lovgrundlag	LBK nr 316 af 05/04/2017 §1, BEK nr 1399 af 12/12/2019 §386 og §447.
Supplerende	Vi anser lydniveau som en del af sundt undervisningsmiljø. [1] [3]
Beskrivelse	For at kunne sikre sundt undervisningsmiljø indsamler vi data, der beskriver indeklima.

Tabel 3 **Formål: Personlig undervisningsmiljøvurdering**

Formål	Personlig undervisningsmiljøvurdering
Hjemmel	En opgave i samfundets interesse eller offentlig myndighedsudøvelse.
Lovgrundlag	GDPR Art. 15.
Supplerende	
Beskrivelse	Personer skal kunne se data, der vedrører dem.

Vi vil også gerne vise to andre undervisningsmiljø-vurderinger. En, der er ment til intern brug, og derfor kan have mere detaljeret information, og en mere generel til eksternt brug. Disse formål er henholdsvis beskrevet i tabel 4 og 5. Da begge disse formål bruger samme lovgrundlag, tilføjer vi en supplerende for-tolkning, hvor vi forstår interessenter på to forskellige måder.

Tabel 4 **Formål: Intern undervisningsmiljøvurdering**

Formål	Intern undervisningsmiljøvurdering
Hjemmel	En opgave i samfundets interesse eller offentlig myndighedsudøvelse.
Lovgrundlag	LBK nr 316 af 05/04/2017 §6 og §7.
Supplerende	Man skal have en forbindelse til skolen, hvor data bliver optaget, for at være interessent.
Beskrivelse	Når vi begrænser, hvem vi vurderer at være interessenter, så kan vi udgive en mere specifik undervisningsmiljøvurdering.

Tabel 5 **Formål: Ekstern undervisningsmiljøvurdering**

Formål	Ekstern undervisningsmiljøvurdering
Hjemmel	En opgave i samfundets interesse eller offentlig myndighedsudøvelse.
Lovgrundlag	LBK nr 316 af 05/04/2017 §6 og §7.
Supplerende	Man ikke skal have en forbindelse til skolen, hvor data bliver optaget, for at være interessent.
Beskrivelse	Når vi ikke begrænser, hvem vi vurderer at være interessenter, så har vi mulighed for at udgive en mere generel undervisningsmiljøvurdering.

Dataabstraktioner:
Hvordan bliver data beriget eller abstraheret

Vi har tidligere talt om, at vores data kan tage flere forskellige former, selv om de har samme kildedata. Data kan også eventuelt beriges med andre data, eller abstraheres via tekniker som aggregering eller anonymisering. Vi kalder disse forskellige former for bearbejdet data for dataabstraktioner.

Hvis borgeren skal kunne forstå, hvordan deres data bliver behandlet, må det stå klart, hvordan deres data indgår i disse dataabstraktioner. Dette inkluderer, hvilke teknikker og data, der bliver brugt til at berige, aggregere eller abstrahere data. Det skal være klart, hvilke data dataabstraktionen ender med at indeholde, samt hvilke formål der giver adgang til brug af dataabstraktionen:

- Datakilder: Hvor kommer data fra?
- Teknikker: Hvordan bliver data behandlet, beriget, aggregeret etc.?
- Dataindhold: Hvad indeholder vores dataabstraktion?
- Formål: Hvilke formål kan bruges til at tilgå dataabstraktionen.

Herunder viser vi i tre tabeller, hvordan vi kan implementere dette for Climify.

Tabel 6 viser, at vi beriger rå indeklimadata optaget fra sensorer med optagelsestidspunkt og lokation. Vi kan bruge formålene Indeklimajustering og DataIndsigt, der tidligere er defineret.

Tabel 6 **Dataabstraktion: Indeklimadata**

Formål	**Intern undervisningsmiljøvurdering**
Dataabstraktion	Indeklimadata
Datakilder	Sensorer i lokaler indsamler lydniveau, CO_2, Fugt, og Temperatur.
Teknik	Hvert datapunkt bliver registreret imod tid og lokale. (Berigelse)
Dataindhold	CO_2, Lydniveau, Temperatur, Fugt. Alle registreret imod tid og lokale.
Formål	Indeklimavedligehold, Dataindsigt.

De to resterende dataabstraktioner beskrevet i tabel 7 og 8 bruger data fra dataabstraktionen Indeklimadata og aggregerer den på lokaleniveau samt på skoleniveau, og kan henholdsvis behandles med formålet Intern undervisningsmiljøvurdering og Ekstern undervisningsmiljøvurdering.

Tabel 7 **Dataabstraktion: Rumaggregering**

Dataabstraktion	**Rumaggregering**
Datakilder	Indeklimadata
Teknik	Statistiske udtræk imod lokale: Gennemsnitlige klimaværdier under undervisning, per uge. (Aggregering) Ekstremværdier for indeklima under undervisning, per uge. (Aggregering) Antal undervisningstimer per uge, hvor indeklima var uden for acceptable normer. (Aggregering)
Dataindhold	Statistiske udtræk registreret imod tid og lokale.
Formål	Intern undervisningsmijløvurdering.

Tabel 8 **Dataabstraktion: Skoleaggregering**

Dataabstraktion	**Skoleaggregering**
Datakilder	Indeklimadata
Teknik	Statistiske udtræk imod skole: Gennemsnitlige klimaværdier under undervisning, per uge. (Aggregering) Ekstremværdier for indeklima under undervisning, per uge. (Aggregering) Antal undervisningstimer per uge, hvor indeklima var uden for acceptable normer. (Aggregering)
Dataindhold	Statistiske udtræk registreret imod tid og skole.
Formål	Ekstern undervisningsmiljøvurdering.

Politik:
Hvornår må hvilke personer behandle hvilke data?
Når vi har defineret vores dataabstraktioner og hvilke formål, der kan bruges til at behandle dem, mangler der en klar definition af konteksten, hvor behandlingen kan udføres. Vi gør dette igennem adgangskontrolpolitikker, der passer til vores formål.

Hvor formålene afklarer, hvorfor vi må benytte dataabstraktionerne, så afklarer adgangskontrolpolitikerne, hvem vi viser dem til, hvad disse personer må gøre ved disse data, og i hvilken kontekst de kan få adgang. Vi skal altså have besvaret følgende spørgsmål:

- Politik: Hvilket formål gælder denne politik for?
- Hvem: Hvem må få adgang til dataabstraktion(en/erne)?
- Hvad: Hvilke dataabstraktioner kan de se?
- Hvordan: Hvilken handling må data indgå i?
- Hvornår: I hvilken kontekst får de adgang?
- Klartekst: Politikken forklaret kort og præcist.

Hvem må få adgang til dataabstraktionerne? Det skal stå klart, om det er en gruppe personer, f.eks. elever på ungdomsuddannelser, deres forældre, eller personer med et specifikt ansvar som en indeklimaansvarlig. Hvilke dataabstraktioner drejer det sig om? Må de få adgang til rå indeklimadata eller aggregeret data for skoler? Hvordan må de anvende data? Må de slette data eller kun læse i dem? Under hvilke omstændigheder må personerne behandle data? Skal de selv have været i rummet, da data blev indsamlet - eller skal de specifikt have ansvar for indeklimaet på skolen, hvor data er opsamlet?

Vi beslutter, at indeklimaansvarlige må få adgang til data fra de skoler, hvor de er ansvarlige for klimajustering i tabel 9.

Tabel 9 **Politik: Indeklimajustering**

Politik	Indeklimadata
Hvem	Klimaansvarlig
Hvad	Indeklimadata
Hvordan	Læse
Hvornår	Når den indeklimaansvarlige har ansvar for indeklimaet på den skole, hvor data er indsamlet.
Klartekst	Den indeklimaansvarlige må læse indeklimadata, hvis personen har ansvar for indeklimaet på den skole, hvor indeklimadata stammer fra.

Tilsvarende må personer, der har været i rummet, da indeklimadata blev indsamlet, få adgang til at læse denne indeklimadata ud fra reglerne om Dataindsigt, som beskrevet i tabel 10. Hvis man er formynder for denne person, må man også få adgang til data, som beskrevet i tabel 11.

Tabel 10 **Politik: Personlig undervisningsmiljøvurdering**

Politik	Personlig undervisningsmiljøvurdering
Hvem	Person
Hvad	Indeklimadata
Hvordan	Læse
Hvornår	Når personen har været til stede i et lokale på samme tidspunkt, som data er blevet indsamlet i lokalet.
Klartekst	En person har ret til at se indeklimadata, hvis personen har været til stede i et lokale på det tidspunkt, hvor data er blevet indsamlet i lokalet.

Tabel 11 **Politik: Personlig undervisningsmiljøvurdering (Formynder)**

Politik	Personlig undervisningsmiljøvurdering
Hvem	Person
Hvad	Indeklimadata
Hvordan	Læse
Hvornår	Når en person er formynder for en person, der har været til stede i et lokale på et tidspunkt, hvor der er indsamlet indeklimadata i samme lokale.
Klartekst	En person har ret til at se data, hvis personen er formynder for en person, der har været til stede i lokalet samtidig med, at indeklimadata blev indsamlet i samme lokale.

Elever, ansatte og kommunalt ansatte må gerne læse Rumaggregering, hvis de har en forbindelse til skolen, hvor data blev optaget, som defineret i tabel 12.

Tabel 12 **Politik: Intern undervisningsmiljøvurdering**

Politik	Intern undervisningsmiljøvurdering
Hvem	Elever, ansatte, kommunalt ansatte
Hvad	Rumaggregering
Hvordan	Læse
Hvornår	Personer med relation til en skole har ret til at se Rumaggregering fra skolen.
Klartekst	Ansatte, kommunalt ansatte og elever kan læse Rumaggregering, hvis de har relation til skolen og den interne undervisningsrapport omhandler netop skolen.

Den sidste politik omhandler en Ekstern undervisningsmiljøvurdering – defineret i tabel 13, hvoraf det fremgår, at enhver person må se Skoleaggregering, når det netop handler om overordnede tal for skolen i forhold til undervisningsmiljøvurdering.

Tabel 13 **Politik: Ekstern undervisningsmiljøvurdering**

Politik	Ekstern undervisningsmiljøvurdering
Hvem	Person
Hvad	Skoleaggregering
Hvordan	Læse
Hvornår	Altid
Klartekst	Alle personer har ret til at se en samlet opgørelse over skolens indeklima.

Håndbog i Smart City Privacy

Dermed har vi klarlagt reglerne for persondata-håndtering i Smart City-projekter. Benyt håndbogen som tjekliste og udfyld de følgende tjeklistesider som udgangspunkt for klarlægningen af jeres egne projekter.

Der er også udgivet en Håndbog i smart city sikkerhed, som kunne være til inspiration.

Den kan downloades her:

Referencer

[1] BrancheFællesskabet for Arbejdsmiljø for Velfærd og Offentlig administration. Støj i skolen, 2018. https://www.arbejdsmiljoweb.dk/media/o2uehuao/stoej-i-skolen 2018 web.pdf.

[2] Datatilsynet. Vejledning om de registreredes rettigheder, 2018. https://www.datatilsynet.dk/media/7582/registreredes-rettigheder.pdf

[3] Maria Klatte, Kirstin Bergström, and Thomas Lachmann. Does noise affect learning? A short review on noise effects on cognitive performance in children. Frontiers in psychology, 4:578, 2013.

[4] Undervisningsministeriet. Bekendtgørelse af lov om elevers og studerendes under visningsmiljø, 2017. https://www.retsinformation.dk/Forms/R0710.aspx?id=188636.

[5] Undervisningsministeriet. Bekendtgørelse om bygningsreglement 2018 (br18)), 2019. https://www.retsinformation.dk/eli/lta/2019/1399.

[6] Datatilsynet. Hvad er personoplysninger? https://www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber-/hvad-er-personoplysninger

Tjekliste til håndtering af persondata
– download skemaer her

Tjekliste til håndtering af persondata

Tabel 1 **Hvornår, hvem får adgang til hvilke data**

Subjekt	Formål	Udstillet Data
Offentligheden		
Ansatte/Kommune		
Ansvarlige for		
Person på stedet		

Tabel 2 **Formål: X**

Formål	
Hjemmel	
Lovgrundlag	
Supplerende	
Beskrivelse	

Tabel 3 **Dataabstraktion: Overordnet om projekt**

Dataabstraktion	
Datakilder	
Teknik	
Dataindhold	
Formål	

Tabel 4 **Politik: Overordnet om projekt**

Politik	
Hvem	
Hvad	
Hvordan	
Hvornår	
Klartekst	

Ordforklaring

Anonyme data og anonymisering
Anonyme data er data, hvor man ikke kan genkende personer ud fra oplysningerne – heller ikke i kombination med andre oplysninger.

Anonyme data er ikke underlagt persondataforordningen, GDPR. Anonymisering er en vigtig øvelse i forhold til at kunne indsamle vigtig og brugbar information om personer.

Anonymiseringsmetoder:
Pseudonymisering og aggregering
Datatilsynet definerer pseudonymisering som "behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person". [6] Så længe pseudonymisering foregår som ovenstående, vil den sikre borgeren anonymitet.

Ved aggregering samler man oplysninger i grupper, så der ikke er fokus på et enkelt individ. Det kan f.eks. være et antal personer inden for et geografisk område. Aggregerede oplysninger er alene anonyme, såfremt personerne ikke kan genkendes ud fra oplysningerne eller ved at kombinere andre oplysninger med de aggregerede.

Dataabstraktion
Den samme information kan eksistere i forskellige former, med forskellig specificitet. Dette kunne være information om, at en person har været et sted på et bestemt tidspunkt. F.eks. at person x var i lokale 1.12B klokken 13:45, og person x var i bygning 12 mellem klokken 13 og 14. Vi kalder disse forskellige former af samme information for dataabstraktioner.

Data kan også eventuelt beriges med andre data, eller abstraheres via tekniker som aggregering eller anonymisering. Vi kalder disse forskellige former for bearbejdet data for dataabstraktioner.

Der er mange måder at bruge dataabstraktioner til at anonymisere eller pseudonymisere data, men de mest oplagte relaterer til tid og sted. Ved at vælge at rapportere måledata ved hjælp af reduceret opløsning kan man vise resultatet af flere målinger i den samme dataværdi.

Devices i smart cities
Sensorer og lignende devices – også kaldet IoT – Internet of Things, indsamler og sender data via netværksteknologier (såsom Wi-Fi, 3/4/5G, Bluetooth, etc.) til databaser og systemer.

Realtidsdata
Realtidsdata er data, der er tilgængelig direkte efter, de er indsamlet. F.eks. kan positionen for plæneklipper, droner og biler overvåges i realtid og overføres til et planlægningsværktøj. Kommunerne efterspørger stadig mere af den type data, og i fremtiden vil flere og flere automatiserede handlinger være baseret på realtidsdata. Det kræver stort fokus på sikkerhed og privacy i sin IoT-infrastruktur.

Server
En server er grundlæggende en computer-ressource, der kan deles mellem autoriserede brugere (kaldet klienter) i et net. Serveren kan bl.a. bruges til lagring af data eller til kommunikation med andre operatører i et netværk. I dag opbevares data ofte i en cloud.

Sikker og Anvendt Data
– et tværkommunalt samarbejde

978-87-643-2004-6