TMF Stab
Teknik- og Miljøforvaltningen

Bilag til xxx

Privacy og juridisk compliance i innovationsforslaget

1. juli 2020

Sagsnummer
2020-0148451

Dokumentnummer
2020-0148451-1

Formålet med innovationsforslaget (pilotprojektet) er bl.a. at trykprøve, om det er muligt at effektivisere udvalgte processer ved brug af ny teknologi uden at gå på kompromis med beskyttelsen af privatlivets fred.

Nedenfor gennemgås forvaltningens overvejelser samt de metoder, som forvaltningen vil anvende i forhold til at sikre borgerens privatliv og rettigheder ifm. innovationsforslaget. Indledningsvis defineres begrebet "privacy".

1. Hvad er privacy?

I EU har politikerne fastslået retten til privatlivets fred i det europæiske charter om fundamentale rettigheder fra år 2000, hvor det i artikel 8 lyder: *"Enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende"*.

Tilsvarende i den europæiske menneskerettighedskonvention fra 1950, hvor det i artikel 8 lyder: *"Enhver har ret til respekt for sit privatliv, sit hjem og sin korrespondance"*, hvilket er inspireret af FN's verdenserklæring om menneskerettigheder fra 1948, artikel 12: *"Ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem og korrespondance"*.

Privatlivets fred er ligeledes sikret i Danmarks Riges Grundlov § 72, hvoraf fremgår: "*Boligen er ukrænkelig. Husundersøgelse, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse.*"

Privatlivets fred er således en fundamental rettighed for danske samt europæiske borgere. Databeskyttelsesforordningens regler skal ses i forlængelse af disse fundamentale rettigheder. Man kan sige, at databeskyttelsesforordningen operationaliserer en grundlæggende rettighed, som er fastslået af EU.

Privacy omtales ofte som individernes (borgernes) autonomi. Det forhold, at man selv kan bestemme, hvad man vil dele med hvem, giver

TMF Stab
Digitalisering
Njalsgade 17, 3.
Postboks 457
2300 København S

EAN-nummer
5798009809452

borgerne autonomi. Det vil være en præmis for gennemførelsen af innovationsforslaget, at der indtænkes privacy i alle løsningerne. Sikkerhed er tæt knyttet til privatlivets fred. Man kan godt have sikkerhed uden privacy, men man kan ikke have privacy uden sikkerhed. Privatlivets fred sikrer, at borgerne får mulighed for at lave deres egne individuelle risikovurderinger og selv bestemme, hvilken risiko de vil løbe, når de behandler – f.eks. overlader eller offentliggør – deres personoplysninger.

Hvis borgerne skal kunne lave sådanne risikovurderinger forudsætter det imidlertid dels, at de ikke er tvunget til at afgive deres personoplysninger (og altså har et reelt frit valg til at vurdere risici), og dels at det er gennemskueligt, hvad de frivilligt afgivne personoplysninger bruges til (så borgerne reelt kan vurdere risikoen). Hvis disse to betingelser er opfyldt kan privatlivets fred bruges til rationelt at optimere borgernes sikkerhed ud fra egne præferencer. Hvis betingelserne ikke er opfyldt, tager andre sikkerhedsmæssige beslutninger på borgernes vegne og sætter borgernes dømmekraft ud af spil – altså en sikkerhedsmæssig umyndiggørelse.

Dette er Teknik- og Miljøforvaltningen meget opmærksom på og har indarbejdet dette i innovationsforslaget.

2. Trussels- og risikobillede

I takt med fremkomsten af nye teknologier, at individer efterlader digitale spor alle steder m.v., så ændrer trusselsbilledet sig også. Ondsindede aktører bliver mere professionelle, finder nye sårbarheder og udnytter dem, f.eks. ift. infrastruktur. I pilotprojektet vil det anvendte udstyr og tjenester som udgangspunkt være sårbare på den ene eller anden måde, enten i forhold til fortrolighed og integritet (hvis udstyret hackes), eller i forhold til tilgængelighed (f.eks. overbelastning eller hærværk af udstyret). Disse risici vil på baggrund af en risikovurdering blive håndteret (f.eks. ved konfigurationen af udstyret og minimering af de data, der indsamles), så sikkerhedsrisiciene nedbringes til et acceptabelt niveau.

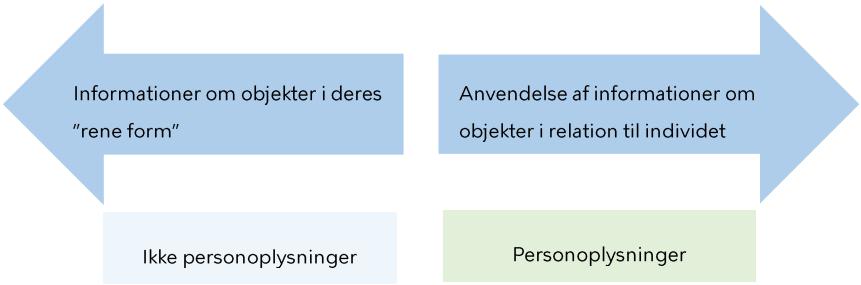
Det tekniske design af løsningerne i pilotprojektet samt risikostyring, herunder databeskyttelse ved design (privacy by design) og konsekvensanalyser, er en central del af svaret på, hvordan Teknik- og Miljøforvaltningen vil håndtere trussel- og risikobilledet.

3. Forvaltningens overvejelser ift. sikring af privacy

Baggrunden er et ønske om at effektivisere forvaltningens processer, så de bliver mere omkostningseffektive og leverer et bedre og mere præcist output, uden at der gås på kompromis med privacy.

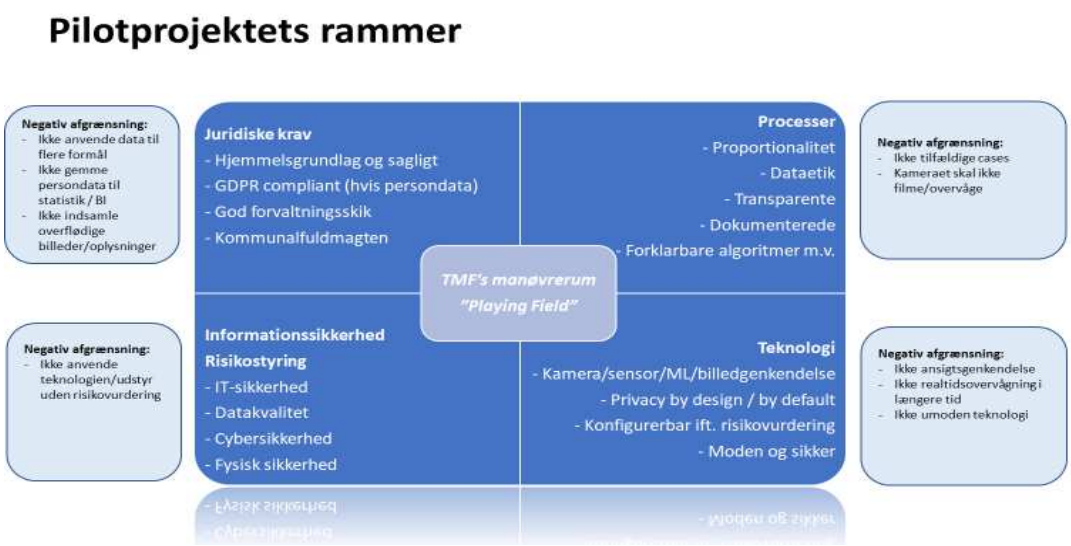
3.1. Behandlingen af personoplysninger i pilotprojektet er minimal
Det er vigtigt at understrege, at omdrejningspunktet for pilotprojektet og de forventede effektiviseringer ikke er personoplysninger, men derimod oplysninger/billeder om objekter (containere m.v.).

Hvis der behandles informationer om objekter i deres "rene form", så er der ikke tale om personoplysninger. Hvis informationerne derimod anvendes om objekter i relation til en borger, vil der være tale om personoplysninger:



De eneste personoplysninger, som vil blive behandlet i de indledende faser i pilotprojektet, er den marginale del af de billeder, som vil blive indsamlet til brug for træning af algoritmen, hvorpå der kan være personer. Ligeledes vil de få billeder med personer, som tilfældigt opholder sig tæt ved en container på det tidspunkt, hvor der tages et billede i forbindelse med den praktiske afprøvning være personoplysninger. Hertil skal det bemærkes, at ansigterne/identiteten på personen vil blive sløret ved en automatisk proces i forbindelse med træningen af algoritmen og den praktiske afprøvning.

3.2.Pilotprojektets rammer
De rammer, som Teknik- og Miljøforvaltningen vil arbejde inden for kan illustreres således:



Eksempel på en proces, som pilotprojektet vil teste:

"Effektivisering af arbejdsgang ved anvendelse af billeder taget med kameraer monteret på kørende driftsmateriel og automatisk billedgenkendelse via machine learning ["ML"]."

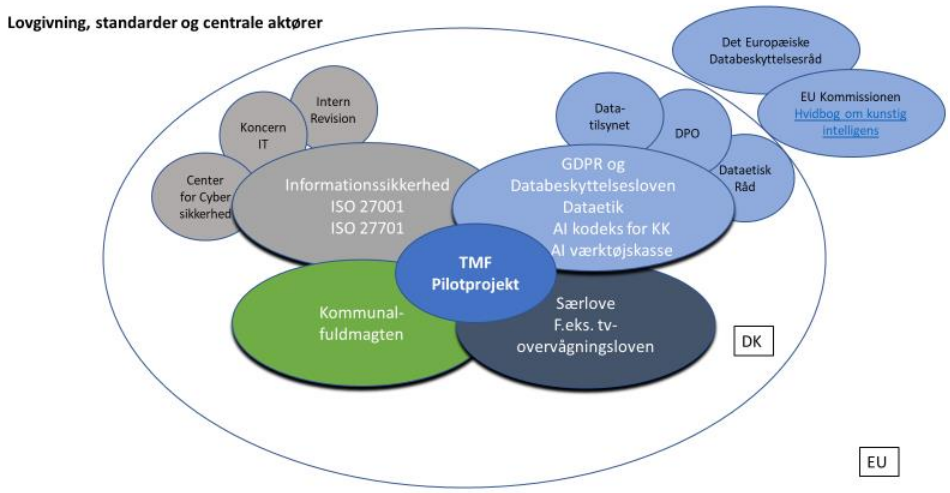
3.3. Overblik over pilotprojektets faser

Faser	Dataindsamling (billeder)	Træning af model/algoritme	Praktisk afprøvning af cloud og edge computing	Grundlag for at træffe valg
Juridisk behandlingsgrundlag	*GDPR Art. 5, art. 6, stk. 1, litra e*	*GDPR Art. 5, art. 6, stk. 1, litra e og stk. 4.*	*GDPR Art. 5, art. 6, stk. 1, litra e*	*GDPR Art. 24, art. 25 og art. 32*
Dataorienteret designprincip	*Minimér og begræns*	*Separér*	*Skjul og beskyt*	*Databeskyttelse gennem standardindstillinger*
Eksempler på privacy by design	*Sløring Maskering Høj opløsning Kryptering Geografisk afgrænsede områder*	*Træning af algoritmen* *Sletning af billeder så hurtigt som muligt*	*Sløring Maskering Geografisk afgrænsede områder Zoom på objekt*	*Forslag til design af konkrete sikkerheds- og privacyløsninger*
Indgår der personoplysninger?	*Der indsamles ml. 40.000-80.000 billeder af containere. På en mindre del af billederne kan der være personer, som har opholdt sig meget tæt på containeren*	*Billeder hvor der indgår personhenførbare oplysning sløres og originalbilleder slettes* *Efter træning slettes alle original bileder*	*Der vil i yderst begrænset omfang kunne blive taget billeder af de personer, som opholder sig tæt på en container på det meget geografisk begrænsede område, hvor*	*Nej, der indgår ikke personoplysninger i leverancerne i pilotprojektet*

			afprøvningen foregår.	

4. Metoder til sikring af juridisk compliance og privacy

Gennemførelsen af pilotprojektet kræver, jf. den præsenterede projektorganisation, inddragelse af juridiske kompetencer ift. kommunalfuldmagtsreglerne, GDPR, tv-overvågning og relevant særlovgivning.



TMF vil beskrive, analysere og dokumentere de juridiske overvejelser og sikre tilstrækkelige beslutningsgrundlag, så Teknik- og Miljøforvaltningen ikke bevæger sig uden for de retlige rammer.

Juridiske barrierer fremhæves i kunstig intelligens (AI)-projekter både som forklaring på manglende konvertering af pilotprojekter til drift og som en strukturel udfordring i organisationernes generelle arbejde med nye teknologier.

Dette er en af årsagerne til, at Teknik- og Miljøforvaltningen ønsker at gennemføre et pilotprojekt samt opbygge kompetencer og erfaringer til at kunne vurdere, om pilotprojektet kan videreføres i driften.

Nogle af de juridiske barrierer ift. pilotprojektet/machine learning vedrører:

- cloudplatforme.
- spørgsmål om, hvordan samarbejdet med offentlige eller private organisationer bør foregå, herunder tvivl om, om partnerskaber kan indgås uden konkurrenceforvridning, og rettighedsspørgsmål vedrørende de løsninger, der er udviklet under eventuelle partnerskaber.

- transparens, ansvar og datasikkerhed.

4.1. Efterlevelse af kravene i databeskyttelsesforordningen
Databeskyttelsesforordningen og databeskyttelsesloven er essentielle værktøjer til at sikre, at borgere har bedre kontrol over deres personlige data, og at disse data bliver behandlet på en legitim, fair og transparent måde.

To retlige krav, der er helt centrale og særligt relevante for pilotprojektet, idet omfang der behandles personoplysninger, er kravet om indbygget databeskyttelse (privacy by design) og pligten til at udarbejde en konsekvensanalyse vedrørende databeskyttelse. Dvs. en analyse af eventuelle konsekvenser for de registrerede (borgere) i forhold til den behandling af personoplysninger, der sker i den pågældende løsning.

Databeskyttelse gennem design og standardindstillinger (art. 25)
Databeskyttelse gennem design indebærer, at Teknik- og Miljøforvaltningen som dataansvarlig allerede fra tidspunktet, hvor teknologien til brug for understøttelsen af behandlingen af personoplysninger fastlægges, skal gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på at sikre en effektiv implementering af de grundlæggende databeskyttelsesprincipper:

Princip	Indhold
Lovlighed, rimelighed og gennemsigtighed	Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede
Formålsbegrænsning	Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål
Dataminimering (proportionalitet)	Personoplysningerne skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles
Rigtighed	Personoplysninger skal være korrekte og om nødvendigt ajourførte, der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges
Opbevaringsbegrænsning	Personoplysningerne skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvor de pågældende personoplysninger behandles

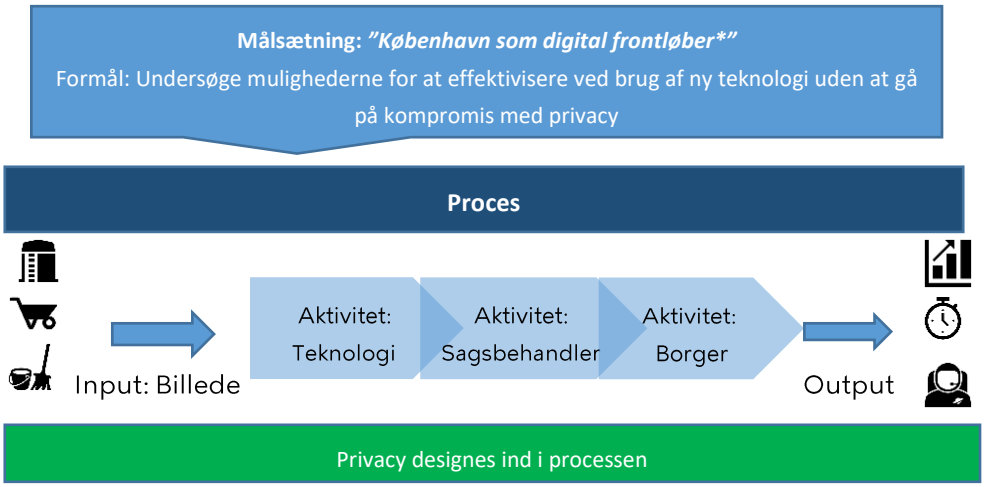
Integritet og fortrolighed	Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.
Ansvarlighed	Den dataansvarlige er ansvarlig for og skal kunne påvise, at de ovennævnte grundprincipper efterleves.

Teknik- og Miljøforvaltningen skal på forhånd have designet og indrettet den teknologiske, it-mæssige og organisatoriske forretningsunderstøttelse af behandlingen af personoplysninger sådan, at databeskyttelsesforordningens krav og beskyttelseshensyn varetages som en integreret del i hele processen.

Eksempler på foranstaltninger, der kan indbygges og udgøre databeskyttelse gennem design, kan være, men er ikke begrænset til:

- Minimeringen af persondatabehandlingen
- Pseudonymisering af personoplysninger så hurtigt som muligt
- Transparens hvad angår personoplysningernes funktion og behandling
- Kryptering af data i transit eller hvile
- Sikring af infrastrukturen mod uautoriseret indtrængen
- Effektive organisatoriske kontroller til autorisation og styring af adgangsrettigheder
- Udladelse af visning af oplysninger i brugergrænseflader, når disse ikke er nødvendige for en given behandling.

Teknik- og Miljøforvaltningen vil i pilotprojektet designe privacy ind i alle delprocesser og i de systemer, som anvendes:



*Der henvises til Digitaliseringsredegørelsen for 2019

Konsekvensanalyser vedr. databeskyttelse
Teknik- og Miljøforvaltningen ønsker, at løsningerne i pilotprojektet gennemgår et dokumenteret privacytjek, inden de igangsættes.

Den metode, som anvises i databeskyttelseslovgivningen, hedder en konsekvensanalyse (Data Protection Impact Assessment). En konsekvensanalyse vedrørende databeskyttelse er en struktureret og dokumenteret proces, der har følgende formål:

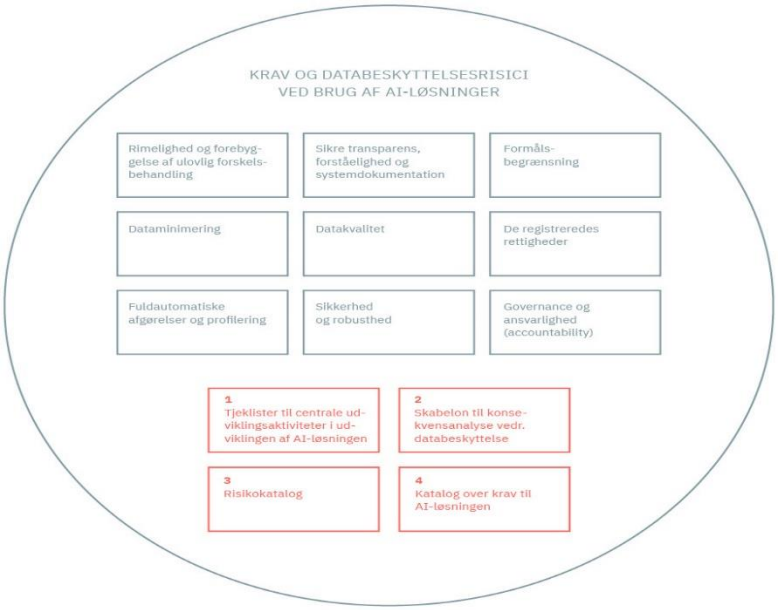
1. Beskrive behandlingen af personoplysninger,
2. vurdere behandlingens nødvendighed og proportionalitet, og
3. bidrage til håndtering af de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen giver anledning til, ved at vurdere dem og fastlægge foranstaltninger til at afhjælpe dem.

Konsekvensanalysen udgør en hjørnesten i pilotprojektet, fordi den er en væsentlig forudsætning for overholdelse af databeskyttelsesforordningens grundlæggende princip om ansvarlighed – dvs. dokumentation for overholdelse af databeskyttelsesforordningens og -lovens regler og principper.

Konsekvensanalysen har en naturlig sammenhæng med databeskyttelsesforordningens krav om databeskyttelse gennem design, da gennemførelsen af konsekvensanalysen ofte giver værdifuldt input til fastlæggelse af krav til databeskyttelsen samt bidrager til, at der tages højde for databeskyttelsesreglerne fra start.

Juridisk AI-værktøjskasse
Der er i regi af en KL arbejdsgruppe med deltagelse af Kammeradvokaten udarbejdet en AI-værktøjskasse, som har til formål at understøtte, at kommunerne kan overholde og håndtere de væsentligste juridiske krav og risici vedrørende databeskyttelse ved udvikling og anvendelse af AI-løsninger i hele AI-løsningernes livscyklus. Arbejdsgruppen er ved at lægge sidste hånd på værktøjerne.

Værktøjskassen har særligt fokus på databeskyttelse gennem design og konsekvensanalyser og indeholder konkrete værktøjer i form af tjeklister, skabeloner, risiko- og kravkatalog m.v. til identifikation og håndtering af de databeskyttelsesretlige krav og risici.



Figur: Emner og værktøjer i den juridiske AI-værktøjskasse.

Teknik- og Miljøforvaltningen vil i pilotprojektet benytte værktøjerne i den juridiske AI-værktøjskasse og få værdifulde erfaringer herfra.

5. Negativ afgrænsning

Nedenfor er et overblik over de positive og negative afgrænsninger i pilotprojektet:

Teknik- og Miljøforvaltningen vil:	Teknik- og Miljøforvaltningen vil ikke:
Arbejde metodisk, risikobaseret og eksplorativt inden for de rammer, som TMF har fået Løbende risikovurdere ift. privacy, og sørge for at nedbringe de risici, der måtte opstå undervejs. TMF vil stoppe pilotprojektet, hvis det mod forventning viser sig, at der er for høje privacyrisici.	Have en stor risikoappetit Fortsætte pilotprojektet, hvis der identificeres høje risici for borgerne
Samarbejde med troværdige leverandører, der kan fremvise produkter, der er testede og hvor algoritmerne er trænede	Samarbejde med leverandører, som andre har anbefalet uden at risikovurdere dem Samarbejde med leverandører, som vil bruge TMF/KK til at produktivisere og teste deres idéer.
Anonymisere og pseudonymisere i videst muligt omfang	Anvende ansigtsgenkendelse Anvende indsamlede data uden at sløre, maskere dem.
Anvende GDPR-compliant teknologi Være opmærksom på alle de danske og internationale standarder og lovgivning, der regulerer privacy, herunder EU's seneste udmeldinger.	Anvende teknologi der er uprøvet, der ikke kan leve op til GDPR-kravene
Samarbejde med relevante aktører, f.eks. privacy eksperter, DTU Compute, Alexandra Instituttet og	Undlade at inddrage den fagekspertise der kræves. Samarbejde med aktører, som ikke har den fornødne ekspertise

forskere, der har erfaring med at designe privacy ind i processer. Inddrage DPO'en i KK og Datatilsynet, hvis det vurderes nødvendigt	
Stoppe konkrete projekter, hvis det viser sig, at der ikke kan opnås et tilfredsstillende privacy-niveau	Bevæge sig ind i en gråzone, hvor det er uklart, om lovgivningen overtrædes. Fortsætte med konkrete pilotprojekter/løsninger, hvis risikovurderingen/konsekvensanalysen viser, at der vil være en høj risiko for borgeren, og denne risiko ikke kan nedbringes

6. Udfordringer og løsninger i pilotprojektet

Minioversigt over de væsentligste udfordringer og forslag til løsninger er nedenfor angivet i ikke-prioriteret rækkefølge:

Udfordring	**Løsninger**
Forvaltningen stirrer sig blind på en konkret teknologi og implementerer den uden et tilstrækkeligt privacy værn.	Gennemføre konsekvensanalyse af databeskyttelsen
TMF vil gerne undgå brugen af personoplysninger	Anvendelse af anonymiseringsteknikker og sikre med processer og teknologi at ikke relevant billedmateriale slettes, herunder det ikke er muligt at lave reverse engineering (dvs. at man ikke kan re-identificere personerne på billederne).
Leverandørerne tilbyder en række produkter, som ikke er gennemsigtige	Lave et kravkatalog til leverandørerne
Kun indsamling af personoplysninger i det omfang det er nødvendigt for at kunne løse den opgave, som er formålet med indsamlingen	Placering af kameraer Anvende anonymiseringsteknikker Maskering af uønskede objekter/mennesker/skygger
Borgerne bliver fotograferet ifm. deres færden i byen	Sløring af ansigter/mennesker på billeder Pilotprojektet gennemføres kun på et afgrænset geografisk område
Dataminimering og sletning	De indsamlede data kun opbevares i så kort tid som muligt. Herefter skal de uigenkaldeligt slettes.

7. Hvorfor skal innovationsforslaget gennemføres nu?

Teknik- og Miljøforvaltningen har overvejet timingen ift. at igangsætte et pilotprojekt med brug af kamera- og sensorteknologi kombineret med machine learning. Teknik- og Miljøforvaltningen har vurderet, at timingen er rigtig nu pga. følgende forhold:

- Der findes nu risikovurderingsværktøjer, som kan vurdere privacyrisici ift. de konkrete løsninger.
- Leverandørerne er modne og klar til at arbejde med privacy by design eller har værdifulde erfaringer hermed. Både i selve produktet og de processer, der knytter sig hertil.
- Teknologien er nu på et tilpas modent stadie og af en så høj kvalitet, at der kan indhøstes værdifulde erfaringer til brug for vurderingen af, om edge computing m.v. kan bruges til tilsyn, dokumentation og kontrol i Teknik- og Miljøforvaltningen.
- Vi kan i Københavns Kommune sætte den standard, vi ønsker både teknisk, juridisk og ikke mindst politisk.