Offentlige myndigheders brug af kunstig intelligens

Inden I går i gang

Oktober 2023

DATATILSYNET

Indhold

Forord

Databeskyttelsesreglerne opfattes sommetider som en hindring for udviklingen af effektive, datadrevne løsninger baseret på nye teknologier som eksempelvis kunstig intelligens ("AI"). Udviklingen af solide, langtidsholdbare AI-løsninger i den offentlige sektor forudsætter dog, at udnyttelsen af det enorme potentiale i data sker med respekt for borgernes grundlæggende rettigheder. Det har databeskyttelsesreglerne netop til formål at sikre.

Efter Datatilsynets opfattelse er innovation og databeskyttelse ikke hinandens modsætninger. Overholdelse af databeskyttelsesreglerne, herunder de centrale principper om bl.a. dataminimering og formålsbegrænsning, er derimod en forudsætning for en demokratisk og hensigtsmæssig teknologisk udvikling af vores samfund. Det fremhæves i forordet til databeskyttelsesforordningen, at et af de primære formål med reglerne er at skabe tillid til myndigheders og virksomheders behandling af personoplysninger.[1] Uden borgernes tillid til, at ny teknologi anvendes ansvarligt og med respekt for deres rettigheder, risikerer ellers lovende løsninger på vigtige samfundsudfordringer at møde modstand og ikke finde fodfæste. Viser I som myndighed, at I efterlever databeskyttelsesreglerne, sender I et tydeligt signal til borgerne om, at der værnes om deres grundlæggende rettigheder, og at de kan have tillid til de teknologiske løsninger, som I stiller til rådighed.

Databeskyttelsesreglerne gælder uanset den valgte teknologi og skal således også overholdes, når personoplysninger behandles ved hjælp af AI. Ved udvikling af AI-løsninger er det vigtigt at tænke databeskyttelse ind allerede i de første faser af projektet. Det kan være meget omkostningstungt og teknisk krævende at tilpasse eller ændre en AI-løsning, f.eks. for at tage højde for en problemstilling om diskrimination eller manglende behandlingsgrundlag, når løsningen er færdigudviklet eller tæt på at være det. Databeskyttelsesreglerne bør derfor altid håndteres som en integreret del af projektforløbet. Dette gælder både før og under udviklingsprocessen samt ved brug af løsningen.

Denne vejledning har til formål at gøre myndigheder i stand til at foretage sig de indledende databeskyttelsesretlige overvejelser, som er en forudsætning for at kunne igangsætte et AI-projekt. Vejledningen er først og fremmest rettet mod de projektansvarlige medarbejdere samt de medarbejdere, der i tilknytning til sådanne projekter rådgiver og vejleder om databeskyttelse.

Vejledningen handler om myndigheders udvikling og brug af AI-løsninger, som primært indebærer behandling af personoplysninger om borgere og eventuelt accessorisk om myndighedernes medarbejdere.

Endelig vedrører vejledningen alene databeskyttelsesreglerne og forholder sig ikke til bl.a. reglerne i EU's kommende forordning om kunstig intelligens. Vejledningen berører heller ikke anden lovgivning såsom forordningen om medicinsk udstyr, sundhedsloven mv.

[1] Præambelbetragtning nr. 6 og 7 til databeskyttelsesforordningen.

1. Hvad er kunstig intelligens?

Der findes endnu ingen præcis og universelt accepteret definition af AI.[2] En række internationale aktører har imidlertid udarbejdet deres egne definitioner af kunstig intelligens. Eksempelvis vedtog OECD i 2019 et sæt principper for kunstig intelligens.[3] Her defineres et AI-system således:

> "*An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy*."

Det forventes også, at EU's kommende forordning om kunstig intelligens, der fortsat er under forhandling, vil indeholde en definition af kunstig intelligens. I EU-Kommissionens forslag til forordningen fra 21. april 2021[4] defineres et AI-system således (udkastets artikel 3, nr. 1):

> "software, der er udviklet ved hjælp af en eller flere af de i bilag I anførte teknikker og tilgange, og som med henblik på et givet sæt mål, der er fastsat af mennesker, kan generere output såsom indhold, forudsigelser, anbefalinger eller beslutninger, der påvirker de miljøer, de interagerer med"

Det Europæiske Råd foreslog i sin generelle indstilling af 6. december 2022 til Kommissionens forslag[5] i stedet denne definition:

> "et system, som er udformet med henblik på at fungere med elementer af autonomi, og som på grundlag af data og input fra maskiner og/eller mennesker udleder, hvordan et givet sæt mål kan nås ved hjælp af maskinlæring og/eller logiske og vidensbaserede tilgange, og som producerer systemgenereret output såsom indhold (generative AI-systemer), forudsigelser, anbefalinger eller beslutninger, der påvirker de miljøer, som AI-systemet interagerer med".

Senest har Europa-Parlamentet den 14. juni 2023 vedtaget sit ændringsforslag til forordningen.[6] Her defineres AI som:

> "et maskinbaseret system, der er designet til at fungere med en varierende grad af autonomi, og som med eksplicitte eller implicitte mål kan generere output såsom forudsigelser, anbefalinger eller beslutninger, der påvirker de fysiske eller virtuelle miljøer."

Meget forenklet er systemer baseret på AI, herunder f.eks. på maskinlæring, systemer, der igennem genkendelse af mønstre og sammenhænge i datasæt kan udlede konklusioner og anvende disse i fremtidige analyser.

I udviklingsfasen trænes et AI-system ved brug af udvalgte datasæt ("træningsdata") til at identificere bestemte mønstre. Systemet bliver derved i stand til at identificere de samme mønstre, når systemet i driftsfasen modtager input i form af nye data. Ved at analysere disse data kan

2 En rapport udarbejdet for EU-Kommissionen har bl.a. undersøgt forskellige definitioner af kunstig intelligens på tværs af 55 forskellige dokumenter, der omfatter bl.a. nationale og internationale strategier og rapporter: AI WATCH. Defining Artificial Intelligence, Publications Office of the European Union: https://publications.jrc.ec.europa.eu/repository/handle/JRC118163

3 OECD, Recommendation of the Council on Artificial Intelligence, C/MIN(2019)3/FINAL.

4 Forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter, COM(2021)206 final: https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A52021PC0206

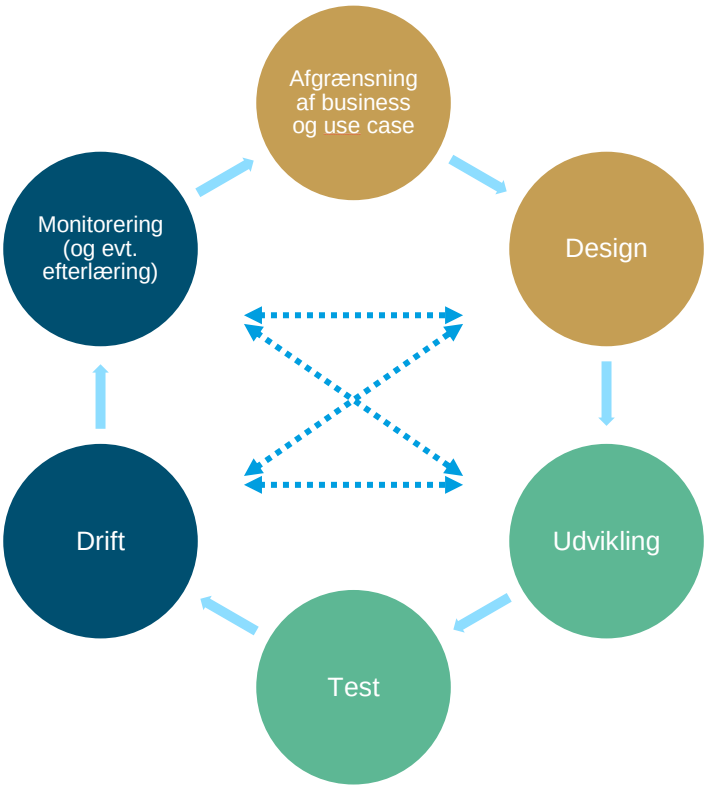
5 Rådet for Den Europæiske Union, Interinstitutionel sag 2021/0106(COD), Forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter – Generel indstilling (den 6. december 2022): https://data.consilium.europa.eu/doc/document/ST-15698-2022-INIT/da/pdf

6 Ændringer vedtaget af Europa-Parlamentet den 14. juni 2023 om forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter, ændring 165: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DA.html

systemet generere output i form af indhold, forudsigelser, anbefalinger eller beslutninger baseret på sandsynligheden for, at et kendt mønster optræder i de nye datasæt.

Set i en databeskyttelsesretlig kontekst er det relevant, men ikke altafgørende, hvorvidt et system skal anses som AI eller ej. Databeskyttelsesreglerne er teknologineutrale, og I skal således overholde reglerne, uanset om I behandler personoplysninger ved brug af AI eller ved brug af et traditionelt it-system. Når det alligevel er relevant at overveje, om et system skal anses som AI, skyldes det, at udvikling og brug af AI kan indebære en særligt omfattende behandling af personoplysninger med deraf følgende risici for borgerne, som I skal identificere og håndtere.

2. Livscyklussen for AI-løsninger



Udvikling og drift af en AI-løsning er typisk en iterativ proces bestående af en række faser, der ikke nødvendigvis sker i en bestemt rækkefølge. En (meget) forsimplet beskrivelse af processen kan ses ovenfor.

1) Afgrænsning af business og use case

Hvis I som myndighed selv ønsker at udvikle en AI-løsning, vil I normalt starte med at identificere et problem, som skal løses, eller en hypotese, som skal undersøges. I denne fase indgår overvejelser om, hvordan I kan opnå det identificerede formål, herunder hvilke typer personoplysninger I skal bruge og hvor mange. Datatilsynet anbefaler, at I allerede i denne tidlige fase også involverer faglige kompetencer, f.eks. sundhedsfaglige, socialfaglige eller lignende, samt juridiske kompetencer, der kan bidrage til at sikre, at systemet er egnet til formålet, effektivt, retvisende og lovligt.

2) Design

En stor del af designfasen for en AI-løsning består i at tilvejebringe fyldestgørende træningsdata. Det kan ske ved at indsamle nye oplysninger eller genbruge eksisterende oplysninger fra egne og eksterne datakilder. I skal almindeligvis foretage en række afgørende juridiske vurderinger, når I udvælger træningsdata. Der vil f.eks. være spørgsmål om, hvorvidt data kan bruges til det påtænkte (nye) formål om at udvikle en AI-løsning, om I kan indhente data hos andre myndigheder til formålet, om borgerne skal orienteres om, at deres oplysninger bruges til dette formål mv. I skal også allerede i denne fase overveje, hvordan udvikling af løsningen kan ske ved brug af færrest mulig personoplysninger.

3) Udvikling og test

Udvikling af løsningen vil ofte ske ved brug af de tilvejebragte træningsdata, men der findes også enkelte AI-modeller, der kan udvikles uden træningsdata. Uanset typen af model, skal I foretage og træffe en række yderligere vurderinger og beslutninger. Det kan vedrøre valg af

AI-model, justering af modellen for at sikre dens statistiske rigtighed og generaliserbarhed[7] samt håndtering af risiko for bias og manglende transparens.

Det vil typisk også være i denne fase, at den udviklede løsning skal testes. I vil her eksempelvis anvende den udviklede løsning på et begrænset datasæt i et kontrolleret miljø med henblik på at teste, om løsningen har brister eller fejl.

4) Drift

Efterfølgende tages den udviklede løsning i brug og indgår i myndighedens daglige drift. Det betyder typisk, at løsningen bruges til at generere indhold og derved bruges som hjælp i driften. Det kan også være, at løsningen genererer forudsigelser eller anbefalinger og bruges som beslutningsstøtte som led i sagsbehandlingen. Endelig kan det være, at løsningen genererer og træffer fuldautomatiske afgørelser over for borgere.

Løsningens output er baseret på de sammenhænge og mønstre, som løsningen har identificeret i træningsdataene, og som løsningen (eventuelt) kan genfinde i de datasæt, som indføres i løsningen, efter den er sat i drift.

Er AI-modellen personoplysninger i sig selv?

Datatilsynet lægger til grund, at en AI-model som et klart udgangspunkt ikke i sig selv udgør personoplysninger, men alene er resultatet af behandlingen af personoplysninger. Det svarer til, at en statistisk rapport ligeledes ikke vil anses som personoplysninger, hvis rapporten alene indeholder konklusioner og aggregerede data, der er resultaterne af den statistiske analyse.

Visse maskinlæringsmodeller kan dog angribes på forskellige måder (såkaldte *model inversion attacks* og *membership inference attacks*), der gør det muligt at re-identificere de borgere, hvis oplysninger har indgået i modellens træningsdata. Et vellykket angreb, som resulterer i re-identifikation af borgernes oplysninger i træningsdata, kan være et brud på persondatasikkerheden og skal håndteres derefter.

Risikoen for, at en ondsindet aktør genidentificerer borgere ved bevidst at gennemføre et angreb for at udlede data, der har indgået i træningsdata, indebærer efter Datatilsynets opfattelse således ikke, at modellen skal anses som personoplysninger i sig selv.

5) Monitorering og eventuelt efterlæring

Når en AI-løsning er taget i brug, skal den løbende monitoreres for at sikre, at dens output bliver ved med at være retvisende. Forpligtelsen til at sikre, at løsningen (fortsat) behandler korrekte personoplysninger og giver retvisende forudsigelser, anbefalinger mv., følger af princippet om rigtighed og kravet om databeskyttelse gennem design og gennem standardindstillinger.[8]

Inden for maskinlæring sondres overordnet mellem statiske og dynamiske modeller. En statisk model udvikles og trænes på udvalgte datasæt, indtil den vurderes klar til at tage i brug. I driftsfasen vil der være behov for jævnlig monitorering af inputdata for at sikre et retvisende output, men modellen ændrer sig ikke ved brug. Idet modellen ikke opdateres løbende, vil dens forudsigelser dog gradvist blive mindre præcise i takt med ændringer over tid i inputdata, f.eks. som følge af den demografiske udvikling. Modellen skal derfor med jævne mellemrum gentrænes for at sikre, at modellens output fortsat er retvisende.

7 Modellens evne til at håndtere nye inputdata og generere korrekte forudsigelser, anbefalinger mv. på samme måde, som det var tilfældet ved træningsdataene.

8 Databeskyttelsesforordningens artikel 5, stk. 1, litra d, og artikel 25.

En dynamisk model (gen-)trænes derimod kontinuerligt på de nye data, den behandler, mens den er i brug. Modellen tilpasser sig således selv løbende og tager højde for eventuelle ændringer, der kommer til udtryk i inputdata. Dette kræver en mere omfattende monitorering for at undgå, at modellen udvikler sig i en uhensigtsmæssig retning. Til gengæld kan modellen løbende forbedres og tilpasse sig ændringer i de underliggende inputdata.

Udviklings- og driftsfaserne vil for en statisk maskinlæringsmodel være mere klart adskilte, mens disse faser i en dynamisk model flyder sammen. Det skal I være særligt opmærksomme på, da det har betydning for de databeskyttelsesretlige overvejelser, inden I sætter et AI-projekt i gang og undervejs.

3. Afgrænsnings- og designfaserne

Når I som myndighed overvejer at udvikle eller indkøbe og sætte en AI-løsning i drift, bør I starte med at besvare to grundlæggende spørgsmål:

1) Hvilke(t) formål skal løsningen bruges til?
2) Hvilke personoplysninger vil blive behandlet via løsningen?

Besvarelsen af disse spørgsmål er en grundlæggende forudsætning for at kunne overholde databeskyttelsesreglerne. Selv i de tilfælde, hvor svaret på ét eller begge spørgsmål forekommer indlysende, anbefaler Datatilsynet, at I som led i afgrænsnings- og designfasen foretager en kortlægning, der på systematisk vis besvarer disse to spørgsmål. Det er Datatilsynets erfaring, at der ofte viser sig at være flere formål med behandlingen, eller at der vil blive behandlet flere typer af oplysninger end oprindeligt vurderet.

Vurderer I på baggrund af denne indledende kortlægning, at jeres AI-løsning lovligt kan udvikles og driftes, skal I desuden være opmærksomme på de øvrige krav, der følger af databeskyttelsesreglerne. Det gælder bl.a. kravet om at sikre proportionalitet igennem hele løsningen, at sikre databeskyttelse gennem design og gennem standardindstillinger og at sikre den fornødne behandlingssikkerhed. Disse krav skal I også overholde gennem hele AI-løsningens livscyklus.

3.1 Formål

Databeskyttelsesreglerne indeholder et generelt krav om, at personoplysninger kun må behandles til et udtrykkeligt angivet og legitimt formål.

I udviklingsfasen af en AI-løsning er formålet, herunder formålet med behandling af personoplysninger, at udvikle en eller flere løsninger. Der bruges typisk historiske oplysninger, som oprindeligt blev indsamlet til et andet formål end udvikling af en AI-løsning, f.eks. konkret sagsbehandling.

Udviklingen af en AI-løsning skal efter Datatilsynets opfattelse anses som et formål i sig selv i konteksten af databeskyttelsesreglerne. Behandling af personoplysninger med henblik på at udvikle nye teknologiske løsninger tjener i sagens natur et andet formål end behandling af personoplysninger som led i myndighedens daglige drift, f.eks. som led i kommunens sagsbehandling eller regionens sundhedsfaglige tiltag over for konkrete borgere. Det gælder også, selv om det langsigtede formål med at udvikle løsningen er at anvende den i myndighedens daglige drift.[9]

Behandling af personoplysninger i forbindelse med henholdsvis udvikling og drift af en AI-løsning indebærer endvidere forskellige vilkår og risici for borgerne.

Borgere vil sjældent opleve direkte konsekvenser af, at deres oplysninger bruges til at udvikle en AI-løsning. Enhver behandling af personoplysninger indebærer dog risici for de borgere, hvis oplysninger det drejer sig om. Ved udvikling af AI-løsninger kan det bl.a. være en risiko for unødvendig dataophobning, da der oftest vil blive genereret særskilte træningsdatasæt baseret på myndighedens eksisterende registre mv. Det kan også være en risiko for, at myndigheden ikke tilvejebringer det samme tilsvarende behandlingssikkerhedsniveau for de træningsdata, som det er tilfældet for produktionsdata.

Endelig vil behandlingen sandsynligvis ikke vil ligge inden for borgernes rimelige forventninger til, hvad myndighederne vil bruge deres oplysninger til.

9 Se i denne retning præmis 40-43 i EU-Domstolens dom af 20. oktober 2022 i sag C-77/21, hvor Domstolen synes at forudsætte, at foretagelse af test og korrektion for fejl af et it-system udgør et separat formål fra opfyldelse af abonnementsaftaler fra kunder, som it-systemet oprindeligt understøttede.

Behandling af borgeres oplysninger i en AI-løsning som led i myndighedens drift vil derimod sædvanligvis indebære større risici for den enkelte borger. Det kan være tilfældet, hvis løsningens output tillægges betydning i en forvaltningsafgørelse eller en beslutning om at iværksætte sundhedsfaglig behandling. Der gælder derfor større krav til denne type behandling.

3.2 Proportionalitet

Når I har fastlagt formålet eller formålene med jeres behandling af borgernes personoplysninger til udvikling af en AI-løsning, skal I vurdere, om behandlingen vil være proportional – det vil sige *egnet, nødvendig og forholdsmæssig* – i forhold til formålet eller formålene. Det følger af princippet om dataminimering.

Umiddelbart kan det synes vanskeligt at forene dette princip med udvikling af AI-løsninger, som generelt kræver behandling af store mængder data, herunder personoplysninger. Det er dog væsentligt, at I holder jer for øje, at dataminimeringsprincippet ikke betyder, at I slet ikke må gøre brug af personoplysninger. I er dog underlagt en forpligtelse til at gøre jer grundige overvejelser om, hvordan I mest hensigtsmæssigt opnår jeres formål – udvikling af en AI-løsning – med brug af alene de oplysninger, som er nødvendige.

I bør i den forbindelse først og fremmest sammenholde det overordnede hensyn til borgerne med de hensyn, der taler for at udvikle og bruge AI-løsningen som led i myndighedsudøvelsen. Med andre ord skal I overveje de fordele for såvel myndigheden som for borgerne, der kan være forbundet med brugen af teknologien. Det kan f.eks. være i form af kortere sagsbehandlingstid, nye behandlingsmuligheder i sundhedssektoren og en mere effektiv udnyttelse af de tilgængelige ressourcer over for de risici for borgernes rettigheder, som brug af teknologien kan medføre.

Når AI-løsningen udvikles, vil borgerne typisk ikke blive direkte påvirket af den behandling af personoplysninger, der sker i denne sammenhæng. Når AI-løsningen derefter sættes i drift, vil løsningen gennem sine forudsigelser, anbefalinger, afgørelser mv., i højere grad kunne påvirke den enkelte borgers sociale, økonomiske, uddannelsesmæssige eller andre typer forhold. I skal derfor forholde jer til proportionaliteten af behandlingen af personoplysninger ved såvel udviklingen som driften af AI-løsningen, som kan indebære forskellige risici for borgerne.

Proportionalitetsvurderingen indebærer dernæst, at I skal overveje, hvordan AI-løsningen kan udvikles, trænes og drives ved brug af færrest mulige personoplysninger – og om muligt helt uden personoplysninger. Databeskyttelsesreglerne indeholder som nævnt ikke et egentligt forbud mod at behandle personoplysninger i forbindelse med udvikling og test af nye teknologiske løsninger, men udgangspunktet er, at der i videst muligt omfang bør anvendes anonymiserede data.

I en AI-kontekst findes der flere teknikker, der kan benyttes for at behandle færre personoplysninger. Det omfatter bl.a. brug af syntetiske data og fødereret læring.[10] Når I udvikler en AI-løsning, skal I overveje brugen af sådanne teknikker allerede i designfasen. I skal gøre jer bestræbelser på at sikre, at I behandler færrest mulige oplysninger ved design og udvikling af løsningen. Der kan være saglige grunde til at fravige dette udgangspunkt, men I skal beskrive, hvorfor udgangspunktet fraviges. Begrundelsen skal bl.a. beskrive, hvorfor det ikke er muligt at brug syntetiske eller anonymiserede data. En begrundelse kunne bl.a. være, at konstruktionen af egnede syntetiske testdata er umulig, eller at der uden brug af personoplysningerne vil være en risiko for, at den kommende løsning vil generere urigtige output efterfølgende. Derimod kan eventuelle omkostninger forbundet med at udvikle f.eks. syntetiske data ikke i sig selv begrunde, at udgangspunktet kan fraviges. Hvis I konstaterer, at dette ikke er muligt, da personoplysninger er nødvendige for udviklingen af AI-løsningen, skal I som det klare udgangspunkt alene anvende pseudonymiserede oplysninger.

10 Det norske Datatilsynet har i regi af deres regulatoriske sandkasse for AI udgivet en rapport om fødereret læring: Finterai, sluttrapport: Maskinlæring uten datadeling | Datatilsynet

3.3 Brug og genbrug af datasæt, herunder fra eksterne datakilder

Udvikling, træning og drift af AI-løsninger forudsætter typisk behandling af større datasæt. Det kan være myndighedens egne datasæt, f.eks. historiske sager, egne registre mv. Det kan også være datasæt hos andre myndigheder, f.eks. BBR, CVR eller patientjournaler hos andre regioner.

Uanset, om I ønsker at bruge egne data eller data fra andre myndigheder, er det vigtigt at være opmærksom på, hvilket formål de pågældende data oprindeligt blev indsamlet til. Det skyldes, at databeskyttelsesreglerne indeholder et krav om, at oplysninger ikke må behandles på ny til et formål, der er uforeneligt med det oprindelige formål.

Reglen indebærer, at data, som I måtte indsamle, ikke frit kan genbruges, videregives mv. I kan således kun genbruge data eller modtage data fra andre myndigheder, hvis jeres nye formål med behandlingen er foreneligt med jeres oprindelige formål. Ligeledes må I kun modtage data fra andre myndigheder, hvis jeres formål med at behandle dataene ikke er uforeneligt med det formål, den afgivende myndighed oprindeligt indsamlede dataene til.

Det er den afgivende myndighed, der skal vurdere, om de omhandlede data vil blive brugt til et foreneligt formål. Det skyldes, at videregivelsen i sig selv udgør en behandling af personoplysninger, og allerede denne behandling må ikke ske til et uforeneligt formål. Hvis en anden myndighed eller virksomhed anmoder jer om data, skal I derfor vurdere det formål, som myndigheden eller virksomheden vil bruge disse data til.

Der er overordnet set to muligheder for myndigheder til at viderebehandle data. For det første kan det ske, hvis viderebehandlingen ikke er uforenelig med det oprindelige indsamlingsformål. For det andet kan de ske, hvis det er fastsat i EU- eller dansk lovgivning.

Uforeneligt med det oprindelige formål

Når I – eller den myndighed, som skal videregive oplysninger til jer – skal vurdere, om jeres (gen)brug af de identificerede datasæt er forenelig med det formål, som datene oprindeligt blev indsamlet til, skal der bl.a. tages hensyn til:

a) enhver forbindelse mellem det formål, som oplysningerne er indsamlet til, og formålet med jeres påtænkte brug
b) den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem jer og borgerne
c) personoplysningernes art, herunder særligt om det drejer sig om særlige kategorier af oplysninger eller oplysninger om strafbare forhold
d) de mulige konsekvenser for borgerne ved jeres påtænkte brug
e) tilstedeværelse af såkaldte fornødne garantier såsom pseudonymisering.

Generelt er der i praksis forholdsvis vide rammer for offentlige myndigheder til at viderebehandle oplysninger til andre formål i modsætning til private aktører, hvor rammerne i praksis er snævrere. Der vil som oftest ikke være noget til hinder for, at oplysninger videregives til andre myndigheder, som har brug for oplysningerne i deres sagsbehandling.

Hvis I ønsker at bruge eksterne data eller give andre mulighed for at bruge jeres data, skal I også være opmærksomme på spørgsmålet om behandlingsgrundlag. En myndighed, der ønsker at give adgang til sine data til f.eks. en virksomhed til brug for virksomhedens udvikling af en AI-løsning, skal have et retligt grundlag for at videregive oplysningerne. Samtidig skal myndigheden til en vis grad påse, at modtageren, f.eks. virksomheden, som oplysningerne videregives til, har et retligt grundlag for at behandle disse oplysninger. Hvis I som myndighed bliver opmærksomme på, at det er usandsynligt, at modtageren har et retligt grundlag for sin behandling af oplysningerne, vil det ikke være lovligt for jer at videregive oplysningerne.

Af eksempler fra Datatilsynets praksis kan nævnes:

Datatilsynets praksis (j.nr. 2006-321-0486)

Udenrigsministeriet anmodede tilsynet om en forhåndstilkendegivelse vedrørende spørgsmålet om, hvorvidt ministeriet på baggrund af oplysninger i et register (modtaget fra politiet), hvori navn og personnummer på evakuerede personer fra Libanon var opført, kunne enten be- eller afkræfte om en bestemt person var opført i registeret over for bl.a. kommuner, der ønskede at kontrollere, om den pågældende person havde begået socialt bedrageri.

Datatilsynet endte med at acceptere, at kommunernes videreanvendelse af personoplysninger med henblik på at kontrollere for socialt bedrageri var foreneligt med indsamlingsformålet, der var at evakuere de pågældende danske statsborgere.

Datatilsynet udtalte således, at Udenrigsministeriet lovligt kunne af- eller bekræfte, om en bestemt person var opført i registret, når blot den anmodende kommune kunne godtgøre, at den havde hjemmel til at foretage en sådan kontrol af enkeltpersoner. Udenrigsministeriet kunne også videregive hele registret til en kommune, der anmodede om det, hvis kommunen selv opfyldte betingelserne for at kunne sammenstille og samkøre personoplysninger i kontroløjemed. Det vil sige, at den modtagende myndighed skulle have et klart og utvetydigt retsgrundlag, som giver lovhjemmel til at foretage sammenstilling eller samkøring i kontroløjemed. – og såfremt myndigheden forudgående havde informeret de persongrupper, der blev berørt af kontrollen, om muligheden for at foretage en generel kontrol.

Det betyder dog ikke, at myndigheder frit kan genbruge egne eller andre myndigheders data. Der er grænser, som også kan genfindes i Datatilsynets praksis:

Datatilsynets praksis (j.nr. 2008-632-0034)

Datatilsynet anmodede Forsvarets Personeltjeneste om en udtalelse, idet tilsynet gennem medieomtale var blevet opmærksom på, at tjenesten havde videregivet personaleoplysninger om 15.000 medarbejdere til forsikringsselskabet Topdanmark.

Forsvarets Personeltjeneste oplyste, at tjenesten som led i en aftale med Topdanmark om ydelse af rabat på forsikringspræmier til medarbejdere i Forsvaret midlertidigt havde videregivet et adresseudtræk til Topdanmark med henblik på udsendelse af tilbud til Forsvarets ansatte. Adresseudtrækket omfattede samtlige ansatte under Forsvarskommandoens myndighedsområde og indeholdt navne, stillingsbetegnelser og adresser.

Datatilsynet var ikke enig med Forsvaret Personeltjeneste i, at videregivelsen kunne ske inden for rammerne af bl.a. formålsbestemthedsprincippet. Datatilsynet lagde i den forbindelse vægt på, at de videregivne oplysninger var indsamlet og behandlet for at administrere et ansættelsesforhold, og at videregivelse til en privat virksomhed med henblik på markedsføring ikke kunne anses som foreneligt med dette formål. Derudover lagde Datatilsynet vægt på, at det ikke kunne antages at stå Forsvarets ansatte klart, at oplysninger, der var blevet afgivet i forbindelse med et ansættelsesforhold, kunne blive videregivet til en privat virksomhed til brug for markedsføring.

Efter Datatilsynets opfattelse har myndigheder – under iagttagelse af de forvaltningsretlige principper om saglighed og ligebehandling – et vidt skøn med hensyn til, i hvilket omfang

myndigheden kan genbruge egne eller andre myndigheders data eller indhente data fra andre myndigheder som led myndighedsudøvelsen.[11]

I skal dog som myndighed være særligt opmærksomme på de tilfælde, hvor I ønsker at udvikle en AI-løsning til brug for samkøring af oplysninger i kontroløjemed. Selvom det – modsat tidligere – ikke længere er en forudsætning, at samkøring af oplysninger i kontroløjemed skal have særskilt hjemmel i en lov, sætter databeskyttelsesreglerne en ramme for, i hvilket omfang samkøring kan finde sted.[12]

Eksempel 1

En statslig myndighed har til opgave at udbetale en lang række offentlige ydelser. Myndigheden skal ligeledes føre kontrol med og bekæmpe fejludbetalinger af og snyd med ydelserne.

Det følger af lovgivningen, som myndigheden arbejder under, at myndigheden kan samkøre oplysninger fra egne registre og oplysninger, der er indhentet fra andre myndigheder, i kontroløjemed.

Myndigheden ønsker nu også at indhente og samkøre oplysninger om borgernes elforbrug i kontroløjemed. Oplysningerne kan indhentes fra Energinet, der er en offentlig virksomhed, som har ansvaret for den såkaldte Datahub. Oplysningerne, der findes i Datahubben, stammer fra elhandelsvirksomhederne, som har indsamlet oplysningerne til afregningsformål og med henblik på at sikre forsyningssikkerheden og kvalitet og kapacitet i elnettet.

Efter Datatilsynets opfattelse er myndighedens ønske om at modtage oplysninger om elforbrug med henblik på samkøring i kontroløjemed et uforeneligt formål med det, som oplysningerne oprindeligt blev indsamlet til, idet myndigheden ikke har et klart retsgrundlag for at indhente oplysninger fra virksomheder.

Myndigheden skal have et klart og utvetydigt retsgrundlag, som giver mulighed for at foretage samkøringen i kontroløjemed, hvilket ikke er tilfældet i myndighedens nuværende lovgivning.

Eksempel 2

En kommune er forpligtet efter serviceloven til at yde støtte til kropsbårne hjælpemidler som korsetter, proteser, ortopædisk fodtøj mv. til borgere, som har varig nedsat fysisk eller psykisk funktionsevne.

Kommunen modtager årligt mange ansøgninger fra borgere, og borgerne oplever lange sagsbehandlingstider. Med henblik på at afhjælpe de lange sagsbehandlingstider beslutter kommunen at udvikle en AI-løsning, der kan fremsøge tidligere lignende sager, som kan understøtte sagsbehandlingen.

Kommunens behandling af borgernes personoplysninger, som fremgår af ansøgningerne, sker med henblik på udførelse af kommunens myndighedsopgave i henhold til serviceloven.

Eftersom udvikling af en AI-løsning må anses som et formål i sig selv, skal kommunen vurdere, om behandling af borgernes oplysninger med henblik på at udvikle en AI-

11 Det er dog uafklaret – og omtvistet i den juridiske litteratur – præcist i hvilket omfang reglerne om formålsbestemthed sætter grænser for myndigheders (gen)brug af egne data og for data, der indhentes fra andre myndigheder. Se hertil Niels Fenger, Forvaltningsloven med kommentarer (2013), s. 782ff.

12 Databeskyttelsesforordningens artikel 5 og 6, stk. 4. Se også afsnit 2.3.2.3.4 i de almindelige bemærkninger til forslag til databeskyttelsesloven (L 68), FT 2017-18, samt justitsministerens svar på spørgsmål nr. 52 fra Folketingets Retsudvalg af 9. februar 2018.

løsning er foreneligt med kommunens oprindelige formål med behandlingen, som er at modtage og behandle ansøgninger om kropsbårne hjælpemidler.

Det er Datatilsynets vurdering, at formålene i dette tilfælde vil være forenelige. Det skyldes bl.a. sammenhængen mellem formålene, idet AI-løsningen skal bruges til at bistå med behandling af samme type sager, som oplysningerne oprindeligt er indsamlet til. Ligeledes medfører brug af de historiske oplysninger til udvikling af løsningen ingen direkte konsekvenser for de borgere, der allerede har modtaget en afgørelse om hjælpemidler.

Fastsat i EU-retten eller dansk ret

I kan også (gen)bruge oplysninger til et nyt formål, hvis det følger af lovgivningen. Det kan være såvel EU-retten som dansk ret. I så fald skal I ikke foretage en selvstændig vurdering af, om det nye formål med at bruge oplysningerne er uforeneligt med det oprindelige formål.

Eksempel 3

En statslig myndighed har til opgave at bistå regionerne med at koordinere fordelingen af elever på gymnasiale uddannelser. Dette vil myndigheden gøre ved brug af en AI-løsning. Elevfordelingen skal bl.a. ske på baggrund af forældrenes indtægtsforhold. Myndigheden indhenter derfor oplysninger om elevernes forældres indkomst- og formueforhold hos skatteforvaltningen.

Det fremgår af lovgivningen, at myndigheden har mulighed for at indhente disse oplysninger hos told- og skatteforvaltningen. Idet (gen)brug af oplysninger om forældrenes økonomiske forhold følger af lovgivning, skal myndigheden ikke konkret vurdere, om behandlingen er forenelig med det oprindelige formål, som begrundede behandlingen af oplysningerne om forældrene (skatteansættelse).[13]

Videnskabeligt eller statistisk øjemed

Hvis I vurderer, at udvikling af jeres AI-løsning sker i videnskabeligt eller statistisk øjemed, vil behandlingen af de nødvendige data ikke være uforenelig med det oprindelige formål. Se nærmere om, hvornår udvikling af AI kan anses for at ske i videnskabeligt eller statistisk øjemed nedenfor i afsnit 4.1.2. Derudover skal I være opmærksomme på, at dette udgangspunkt om forenelighed ikke nødvendigvis gælder for driftsfasen, idet drift som hovedregel ikke længere kan anses for at ske i statistisk eller videnskabeligt øjemed.

Eksempel 4

En myndighed ønsker at opnå mere viden om 21-35-åriges indkomstniveau de sidste tre årtier for at analysere sammenhænge mellem uddannelse og indkomstniveau og eventuelt kunne forudsige fremtidige mønstre herom. I den forbindelse ønsker myndigheden at indhente bl.a. beskæftigelsesoplysninger fra jobcentrene i kommunerne. Eftersom undersøgelsen forudsætter en analyse af store mængder data, vælger myndigheden at udvikle en AI-løsning, som skal foretage den statistiske analyse og udarbejde forudsigelser af fremtidige mønstre.

13 Datatilsynet bemærker, at eksemplet er fiktivt. Datatilsynet er ikke bekendt med, at en sådan AI-løsning anvendes i praksis.

Oplysningerne blev af jobcentrene oprindeligt indsamlet til brug for borgernes konkrete sager på beskæftigelsesområdet og blev således indsamlet til et andet formål end i statistisk øjemed, som er det myndigheden nu ønsker at bruge oplysningerne til.

Idet behandlingen af oplysningerne sker i statistisk øjemed, skal denne viderebehandling ikke anses for at være uforenelig med det oprindelige formål.

Uanset om I selv genbruger data i videnskabeligt eller statistisk øjemed, eller om I videregiver data til andre myndigheder i samme øjemed, skal I fortsat være opmærksomme på kravet om, at data skal behandles til et sagligt og specifikt formål.

Datatilsynets praksis (j.nr. 2022-32-2939)

Datatilsynet modtog en række henvendelser fra borgere, som var utilfredse med, at Rigspolitiet havde videregivet oplysninger om, at de havde modtaget en fartbøde, til Aalborg Universitet til brug for et konkret forskningsprojekt.

Forskningsprojektet handlede om at forebygge hastighedsovertrædelser i trafikken og skulle vise, om bilister får færre fartbøder, hvis de efter at have fået en fartbøde gennemgår en onlinelæring om trafiksikkerhed.

En af henvendelserne til Datatilsynet var fra en borger, der havde gjort indsigelse mod bødeforlægget og afventede domstolenes behandling af sagen.

Datatilsynet fandt, at Rigspolitiet generelt kunne videregive oplysninger om bilisters overtrædelse af færdselsloven til Aalborg Universitet til brug for forskningsprojektet i medfør af databeskyttelseslovens § 10, stk. 1.

Datatilsynet fandt imidlertid også, at Rigspolitiets videregivelse af oplysningerne i det konkrete tilfælde var sket i strid med principperne om formålsbegrænsning og dataminimering, da Rigspolitiets videregivelse ikke var sket til et sagligt og relevant formål.

Datatilsynet lagde i den forbindelse vægt på, at det på tidspunktet for Rigspolitiets videregivelse fortsat måtte anses for at have haft formodningen imod sig, at den pågældende borger havde overtrådt færdselsloven, indtil sagen var blevet afgjort ved domstolene, og at forskningsprojektets målgruppe efter Datatilsynets opfattelse var personer, der har overtrådt færdselsloven.

Som led i udvikling og drift af AI-løsninger kan der i øvrigt opstå flere formål med behandlingen af personoplysninger som følge af de resultater, løsningen leverer. Hvis I som myndighed ønsker at forfølge disse formål, skal I foretage nye vurderinger af bl.a., om disse nye formål er uforenelige, og om I har hjemmel til at forfølge disse formål.

Eksempel 5

En kommune beslutter sig for at udvikle en AI-løsning for at forbedre sin håndtering af aktindsigtsanmodninger med hensyn til svartid, kvalitet og ensartethed. Løsningen skal effektivt kunne fremsøge akter og dokumenter og identificere oplysninger, der skal anonymiseres, og skal understøtte sagsbehandlingen.

AI-løsningen trænes ved brug af data, der stammer fra historiske aktindsigtssager.

Det indebærer, at kommunen viderebehandler personoplysninger, som oprindeligt blev indsamlet til ét formål (sagsbehandling af aktindsigtsanmodninger), til et nyt formål (udvikling af en AI-løsning).

Kommunen skal derfor vurdere, om det nye formål er foreneligt med det oprindelige. Efter Datatilsynets opfattelse er der en naturlig forbindelse mellem behandling af personoplysninger som led i sagsbehandling af aktindsigtsanmodninger og udvikling af et værktøj, der skal understøtte den samme sagsbehandling. Derudover foretages viderebehandlingen af samme myndighed, som oprindeligt har indsamlet oplysningerne.

Det nye formål – udviklingen af AI-løsningen – kan derfor anses for foreneligt med det oprindelige formål.

I skal i øvrigt være opmærksomme på, at behandling af oplysninger til andre formål end de oprindelige medfører, at I skal oplyse borgerne om de(t) nye formål. Se nærmere herom nedenfor i afsnit 4.2 og 5.4.

3.4 Generelt om behandlingsgrundlag

Det er en grundlæggende forudsætning for, at I lovligt kan behandle personoplysninger til et eller flere formål, at I for hvert formål har et såkaldt behandlingsgrundlag. Indledningsvis bør I derfor foretage en samlet vurdering af hele livscyklussen for jeres kommende AI-løsning for at sikre jer, at I har identificeret de(t) nødvendige behandlingsgrundlag og derved lovligt kan udvikle AI-løsningen og tage den i brug efterfølgende.

Når I som myndighed skal vurdere mulige behandlingsgrundlag i en AI-kontekst, bør I således sondre mellem udvikling og træning samt den efterfølgende drift af løsningen. Det skyldes, at udvikling og træning i en databeskyttelseskontekst skal betragtes som et særskilt formål i forhold til den efterfølgende drift.

I udviklingsfasen er formålet med behandlingen at udvikle en eller flere AI-løsninger. I driftsfasen anvendes AI-løsningerne til at løse en eller flere konkrete opgaver i praksis. Formål med behandlingen er i dette tilfælde nærmere knyttet til opgaven, der skal løses. For visse typer af AI-løsninger kan der også være en efterlæringsfase, hvor AI-løsningen videreudvikles og forbedres, mens den er i drift. Her sker en kontinuerlig udvikling af løsningen baseret på oplysninger, der er indsamlet som led i driftsfasen.

Jeres behandling af personoplysninger i disse forskellige faser kan ikke nødvendigvis baseres på det samme behandlingsgrundlag. Det skyldes bl.a., at der kan være stor forskel på de konkrete risici for borgernes rettigheder ved behandlingen i de forskellige faser.

Det vil eksempelvis være tilfældet, hvis I som myndighed køber en AI-løsning hos en leverandør. Leverandøren har sandsynligvis behandlet personoplysninger på baggrund af sin legitime interesse i at udvikle og træne løsningen som et produkt. Når I sætter løsningen i drift, vil I derimod behandle personoplysninger til et eller flere specifikke formål, som I har indkøbt løsningen til. I skal derfor identificere, hvilket behandlingsgrundlag der er relevant for dette formål.

Det kan også være tilfældet, hvis I har udviklet en løsning som led i videnskabeligt øjemed på baggrund af databeskyttelseslovens § 10, og I efterfølgende ønsker at sætte løsningen i drift, f.eks. til brug for patientbehandling.

Hvis I behandler såkaldte særlige kategorier af oplysninger eller oplysninger om strafbare forhold ved brug af AI-løsningen, skal I være opmærksomme på en række yderligere betingelser og krav til behandlingsgrundlaget. I kan læse mere om behandling af særlige kategorier af oplysninger nedenfor i afsnit 3.5.

Ønsker I at bruge AI-løsningen til at træffe automatiske afgørelser, skal I også være opmærksomme på, at der gælder et generelt forbud mod sådanne afgørelser. Brug af automatiske afgørelser forudsætter, at I kan identificere en undtagelse til dette forbud. I kan læse mere herom nedenfor i afsnit 3.6.

I skal altid kende grundlaget for jeres behandling af personoplysninger i en AI-løsning, *før* oplysningerne behandles. I skal kunne dokumentere jeres valg af behandlingsgrundlag og informere borgerne om det. Det betyder også, at I ikke efterfølgende kan ændre

behandlingsgrundlag og eksempelvis skifte fra at behandle oplysningerne på baggrund af et samtykke til et andet retligt grundlag.[14]

3.5 Særlige kategorier af personoplysninger

Behandling af visse personoplysninger er forbundet med en særlig høj risiko for borgeren. Det gælder oplysninger om:

- race eller etnisk oprindelse,
- politisk, religiøs eller filosofisk overbevisning,
- fagforeningsmæssigt tilhørsforhold,
- genetiske data,
- biometriske data med det formål entydigt at identificere en person,
- helbred eller
- seksuelle forhold eller seksuelle orientering.[15]

Af hensyn til den høje risiko for borgernes rettigheder forbundet med behandling af de særlige kategorier af personoplysninger indeholder databeskyttelsesreglerne et generelt forbud mod behandling af disse kategorier af oplysninger. Der kan kun ske undtagelse fra dette forbud i de tilfælde, som fremgår af artikel 9, stk. 2.

Oplysninger kan også være omfattet af denne kategori, selvom de blot kan udledes af den sammenhæng, de indgår i. Om oplysninger skal betragtes som en del af de særlige kategorier af personoplysninger – og dermed omfattet af forbuddet i forordningens artikel 9 – afhænger af, om det er muligt med en høj grad af sikkerhed at afsløre særlige kategorier af oplysninger om en person, eller om man har til hensigt at udlede sådanne særlige kategorier af oplysninger f.eks. ved brug af profilering.[16]

Når I bruger AI, skal I være særligt opmærksomme på, om I behandler særlige kategorier af personoplysninger. Det er i mange tilfælde muligt ved hjælp af AI-løsninger at udlede særlige kategorier af oplysninger ved at sammenstille en række oplysninger om borgerne og på det grundlag drage konklusioner om f.eks. personens fysiske eller mentale helbred, politiske overbevisning eller seksuelle orientering.

I konteksten af AI betyder det, at der kan blive tale om, at I behandler særlige kategorier af personoplysninger, hvis I:

- kan (med en høj grad af sikkerhed) udlede eller har til formål at udlede særlige kategorier af oplysninger om borgerne, eller
- har til formål at behandle borgerne anderledes på baggrund af de udledte særlige kategorier af oplysninger.

Eksempel 6

En kommune har udviklet en AI-løsning, der analyserer GPS- og andre kørselsdata fra hjemmeplejens biler med henblik på at opnå en mere effektiv udnyttelse af de køretøjer, som kommunen har til rådighed.

Som led i sin analyse inddrager AI-løsningen bl.a. adresser, som hjemmeplejen har besøgt. Ud fra disse oplysninger kan der udledes oplysninger om, at borgeren på adressen muligvis modtager hjælp fra hjemmeplejen.

I denne situation behandler AI-løsningen ikke helbredsoplysninger om de pågældende borgere. Det skyldes, at det ikke er muligt med en tilstrækkelig høj grad af sikkerhed

14 Det Europæiske Databeskyttelsesråds retningslinjer nr. 5/2020 om samtykke, s. 27, pkt. 123.

15 Databeskyttelsesforordningens artikel 9, stk. 1.

16 Se også Datatilsynets afgørelse i sagen med j.nr. 2021-31-5478 (Radius Elnet A/S)

at udlede, om – og i givet fald hvilken – form for hjælp de omhandlede borgere modtager fra hjemmeplejen. Derudover har løsningen ikke til formål at behandle borgerne anderledes på baggrund af de analyser, som løsningen foretager. Resultatet af analysen skal alene anvendes til at organisere brugen af hjemmeplejens biler, og der tilsigtes ikke ændringer i indholdet af den service, borgerne modtager.

I kan som offentlig myndighed bl.a. behandle særlige kategorier af personoplysninger, når det er nødvendigt som led i jeres myndighedsudøvelse.

Det kan ske, hvis behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares. Det er bl.a. tilfældet, når I skal vurdere, om borgeren har ret til en ydelse eller om en ansøgning skal imødekommes. Behandling kan både ske med henblik på at fastlægge jeres, borgerens eller tredjemands retskrav.[17]

Behandling af særlige kategorier af oplysninger kan også ske, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser,[18] eller hvis behandlingen er nødvendig til videnskabelige eller statistiske formål.[19] I begge tilfælde kræves et supplerende retsgrundlag, hvor den pågældende behandling er forudsat i lovgivningen. Det er således ikke et decideret krav, at det supplerende retsgrundlag indeholder en udtrykkelig regel om den pågældende behandling.

Kravene, der stilles til klarheden af det supplerende retsgrundlag, afhænger af, hvor indgribende den pågældende behandling er. Behandling af særlige kategorier af oplysninger er forbundet med en særlig høj risiko for borgeren, og der stilles derfor i sagens natur større krav til klarheden af det supplerende retsgrundlag.

Oplysninger om strafbare forhold er ikke blandt de særlige kategorier af oplysninger, der findes i forordningens artikel 9. Der gælder dog også særlige regler for, hvornår I kan behandle den type af oplysninger. I kan som myndighed behandle oplysninger om strafbare forhold, hvis det er nødvendigt for, at I kan varetage jeres opgaver som myndighed.[20]

3.6 Profilering og automatiske afgørelser

3.6.1 Hvad er profilering?

Begrebet ”profilering” dækker over de tilfælde, hvor indsamlede oplysninger anvendes til at lave profiler af en person til at forudse eksempelvis adfærd eller fremtidige behov. Profilering er udtrykkeligt defineret i databeskyttelsesforordningen som ”enhver form for automatisk behandling med henblik på at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.”[21]

AI-løsninger baseret på maskinlæring er særdeles effektive til profilering. Løsningerne er ofte specifikt trænet til at finde bestemte mønstre i datasæt. Når løsningen modtager inputdata, der vedrører en specifik borger, kan modellen generere den statistiske sandsynlighed for, at den pågældende borger f.eks. vil udvise en given adfærd eller udvikle en bestemt sygdom. Sådanne AI-løsninger anvendes bl.a. som beslutningsstøtte for sagsbehandlere i forvaltningen og til billeddiagnostik i sundhedssektoren.

17 Databeskyttelsesforordningens artikel 9, stk. 2, litra f.

18 Databeskyttelsesforordningens artikel 9, stk. 2, litra g.

19 Databeskyttelsesforordningens artikel 9, stk. 2, litra j.

20 Databeskyttelseslovens § 8, stk. 1.

21 Databeskyttelsesforordningens artikel 4, nr. 4.

3.6.2 Hvad er automatiske afgørelser?

Profilering kan – ligesom andre former for behandling af personoplysninger – danne grundlag for afgørelser eller beslutninger vedrørende borgeren. Det kan være i form af beslutningsstøtte, hvor løsningen genererer et forslag eller en anbefaling til afgørelse eller tiltag over for borgeren. Det kan dog også være i form af automatiske afgørelser, hvor løsningen også træffer den beslutning over for borgeren, som løsningen vurderer er rigtigst i den pågældende sammenhæng.

Databeskyttelsesreglerne indeholder et generelt forbud mod afgørelser, "der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende".[22] Forbuddet omfatter således ikke profileringen, men kun automatiske afgørelser (som kan være baseret på profilering). For offentlige myndigheder kan forbuddet umiddelbart kun fraviges, hvis det fremgår af loven, at myndigheden kan træffe sådanne automatiske afgørelser. Samtykke fra borgeren vil almindeligvis ikke kunne fravige dette forbud. Se nærmere om borgernes mulighed for at give samtykke til myndigheder i afsnit 5.2.2.

En særlig problemstilling, som I skal være opmærksomme på, hvis I ønsker at udvikle og bruge en AI-løsning som beslutningsstøtte, er risikoen for såkaldt *automation bias*. Det er tilfælde, hvor f.eks. sagsbehandlere tillægger systemets vurdering af en sag større betydning end deres egen vurdering, hvilket fører til, at systemet derfor de facto afgør sagen. Hvis AI-løsningen fortsat skal betragtes som beslutningsstøtte, skal et menneske selvstændigt have vurderet de oplysninger, der ligger til grund for afgørelsen, og den pågældende skal også have den fornødne autoritet til at tilsidesætte systemets anbefalinger.[23]

Det beror derudover på en konkret vurdering, hvornår en beslutning "på tilsvarende vis betydeligt påvirker den pågældende." Det vil f.eks. være tilfældet med automatiske afslag på banklån eller automatisk frasortering af ansøgere til et job.[24] Beslutninger om at udtrække borgere til kontrolformål, f.eks. på skatte- eller socialområdet, vil i visse tilfælde også kunne påvirke den pågældende i tilstrækkelig grad til at være afgørelser omfattet af artikel 22.[25]

Som det klare udgangspunkt kræves der et klart og præcist lovgrundlag, hvis en myndighed ønsker at træffe automatiske afgørelser eller andre indgribende beslutninger over for borgerne. Det skal fremgå af loven, at myndigheden kan træffe automatiske afgørelser, men det er ikke et krav, at loven specifikt regulerer, at afgørelsen skal ske uden menneskelig indblanding.

22 Databeskyttelsesforordningens artikel 22.

23 Artikel 29-gruppens retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 21f.

24 Præambelbetragtning nr. 71 til databeskyttelsesforordningen.

25 Se nærmere herom Naomi Lindtvedt, Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering, afsnit 3.6.

4. Udviklings- og træningsfasen

En AI-løsnings livscyklus består som nævnt af en række forskellige faser. Det er bl.a. relevant, når I skal identificere et retligt grundlag for jeres behandling af personoplysninger i den pågældende løsning.

Behandling af personoplysninger med henblik på udvikling og træning af løsningen anses efter Datatilsynets opfattelse som et formål i sig selv og adskilt fra de(t) formål, der efterfølgende forfølges med drift af løsningen.

4.1 Relevante behandlingsgrundlag

4.1.1 Opgave i samfundets interesse eller offentlig myndighedsudøvelse

Offentlige myndigheders behandling af personoplysninger med henblik på udvikling og træning af en AI-løsning vil som altovervejende hovedregel ske af hensyn til udførelsen af en opgave i samfundets interesse eller som led i myndighedsudøvelsen.

Hvis I ønsker at udvikle en AI-løsning som led i jeres myndighedsudøvelse, skal I derfor først og fremmest gøre jer klart, hvilke lovregler, bekendtgørelser eller andre administrative forskrifter der forpligter eller bemyndiger jer til at udøve den givne myndighed. I skal med andre ord have mindre fokus på databeskyttelsesreglerne i denne kontekst og undersøge anden relevant lovgivning, som forpligter eller berettiger jer som myndighed til at udføre en bestemt myndighedsopgave.

Sundhedslovens § 222 om Statens Serum Institut

Af bestemmelsen fremgår, at Statens Serum Institut har til formål at forebygge og bekæmpe smitsomme sygdomme, medfødte lidelser og biologiske trusler. Endvidere følger det af bestemmelsen, at Statens Serum Institut fungerer som centrallaboratorium for så vidt angår diagnostiske analyser, herunder referencefunktioner. Instituttet har en national rolle i forhold til varetagelse af landets opgaver i medfør af internationale forpligtelser i relation til grænseoverskridende sundhedsrisici. Instituttet sikrer forsyning af vacciner til de offentlige vaccinationsprogrammer og beredskabsprodukter gennem fremskaffelse, lagring og distribution. Instituttet prioriterer og tilrettelægger distributionen med henblik på at sikre forsyningen og nedbringe risiko for spild af vacciner og beredskabsprodukter. Instituttet indgår i det operationelle beredskab mod smitsomme sygdomme og biologisk terrorisme og beredskabet på det veterinære område. Instituttet driver videnskabelig forskning og yder rådgivning og bistand på områder, som vedrører instituttets opgaver.

Bestemmelsen er et eksempel på en generel bestemmelse om myndighedsudøvelse, som også danner retsgrundlaget for, at SSI kan behandle de personoplysninger, der er nødvendige for at udføre de nævnte opgaver.

Dernæst skal I vurdere, om det relevante lovgrundlag er tilstrækkeligt klart og præcist til at danne grundlag for udvikling af en AI-løsning. Kravet til klarheden af det pågældende lovgrundlag afhænger generelt af, hvor indgribende behandlingen af personoplysninger, der sker som led i udviklingen af AI-løsningen, vil være for borgeren.

Hvis der er tale om en helt harmløs behandling, vil kravene ikke være særlig store. Er der derimod tale om en indgribende behandling, stilles der større krav til klarheden af lovgrundlaget.

Skattekontrollovens § 67 a – et klart retsgrundlag

Told- og skatteforvaltningen kan behandle, herunder samkøre, de oplysninger, told- og skatteforvaltningen er i besiddelse af, for at udvikle it-systemer, der er nødvendige for told- og skatteforvaltningens myndighedsudøvelse.

Derudover kan told- og skatteforvaltningen indsamle og behandle alle nødvendige oplysninger om økonomiske og erhvervsmæssige forhold fra andre offentlige myndigheder og offentligt tilgængelige kilder, herunder samkøre sådanne oplysninger med de oplysninger, told- og skatteforvaltningen er i besiddelse af, med henblik på udvikling af it-systemer, der er nødvendige for told- og skatteforvaltningens myndighedsudøvelse.

Af bemærkningerne til bestemmelsen fremgår:

> ”Den foreslåede bestemmelse indebærer, at Skatteforvaltningen vil kunne foretage samkøring af disse oplysninger med henblik på udvikling af it-systemer, som vil kunne målrette, understøtte og effektivisere Skatteforvaltningens myndighedsudøvelse, når det er nødvendigt. […]
>
> Formålet med den foreslåede bestemmelse i skattekontrollovens § 67 a er i læringsøjemed at udvikle flere forskellige machine learning-modeller og analysemodeller m.v., som på tværs af data vil kunne genkende mønstre og tegn på f.eks. svig. Det bemærkes dog, at principperne om proportionalitet og dataminimering fortsat gælder ved test af data. Det forudsættes derfor, at adgangen til at anvende test ikke benyttes i et videre omfang, end hvad der er nødvendigt for at sikre, at de it-systemer (scoringsmodeller), der vil kunne udvikles efter forslaget, er operationelle og virker efter hensigten. Når de enkelte modeller er udviklet, vil modellerne kunne anvendes med hjemmel i bestemmelsen i skattekontrollovens § 68 om registersamkøring.”[26]

Bestemmelsen er et eksempel på, at der i lovgivningen er fastsat klare rammer for den påtænkte behandling af personoplysninger. Bestemmelsen angiver således, hvilken myndighed der skal behandle personoplysninger og hvilke. Bestemmelsen beskriver også behandlingens karakter (indsamling og samkøring af oplysninger) og formålet hermed (udvikling af maskinlæringsmodeller).

Der gælder efter Datatilsynets opfattelse som udgangspunkt mindre krav til klarheden af det retsgrundlag, der danner baggrund for behandling af personoplysninger til udvikling af en AI-løsning end til selve driften af løsningen. Det skyldes, at risiciene for borgerne ved udvikling af løsningen er mindre, end når løsningen efterfølgende anvendes i sagsbehandlingen, hvor dens databaserede forudsigelser og vurderinger kan få reelle konsekvenser for den enkelte borger.

4.1.2 Forskning og statistik (databeskyttelseslovens § 10)

Databeskyttelseslovens § 10 indeholder et særligt retsgrundlag for behandling af særlige kategorier af personoplysninger og oplysninger om strafbare forhold med henblik på udførelse af statistiske eller videnskabelige undersøgelser. Behandling af andre personoplysninger end de særlige kategorier i statistisk eller videnskabeligt øjemed vil i givet fald ske med henvisning til udførelse af en opgave i samfundets interesse.[27]

26 Uddrag af de specielle bemærkninger til § 3, nr. 1, i lov nr. 2612 af 28. december 2021 om ændring af lov om et indkomstregister, skatteindberetningsloven og skattekontrolloven (Registersamkøring med henblik på systemudvikling og myndighedsudøvelse samt udvidet adgang til eSkatData-ordningen m.v.)

27 Databeskyttelsesforordningens artikel 6, stk. 1, litra e, om udførelse af en opgave i samfundets interesse.

Brug af databeskyttelseslovens § 10 forudsætter, at behandlingen (i) alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser (ii) af væsentlig samfundsmæssig betydning, og (iii) at behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne.[28]

I visse tilfælde kan udvikling af AI-løsninger have en sådan karakter, at udvikling af løsningen kan siges at ske i statistisk eller videnskabeligt øjemed. Det afhænger helt konkret af formålet med udviklingen af den pågældende løsning.

Alene med henblik på at udføre statistiske eller videnskabelige undersøgelser

I må som myndighed vurdere, om den behandling, som I ønsker at foretage i forbindelse med udvikling og træning af en AI-løsning, vil ske med henblik på udførelse af en statistisk eller videnskabelig undersøgelse. I jeres vurdering kan I navnlig inddrage, om udviklingsprojektet vil:

- tilvejebringe ny viden,
- anvende de i den pågældende sektor gældende metodiske standarder,
- efterleve etiske standarder,
- foretages med henblik på at dele forskningsresultater med (dele af) omverdenen, f.eks. med henblik på fagfællebedømmelse og publicering, og
- bidrage til samfundets kollektive viden og trivsel.

Der er ikke tale om en kumulativ eller udtømmende oplistning af kriterier, men alene en række momenter, som kan indgå i den konkrete vurdering, som I skal foretage. Det er dog Datatilsynets opfattelse, at især det førstnævnte forhold – tilvejebringelse af ny viden – og det sidstnævnte forhold – intentionen om at bidrage til samfundets kollektive viden og trivsel – bør tillægges afgørende betydning ved vurderingen af, om en behandlingsaktivitet kan anses som at ske i statistisk eller videnskabeligt øjemed.

Væsentlig samfundsmæssig betydning

For at anvende databeskyttelseslovens § 10 som behandlingsgrundlag skal jeres udviklingsprojektet derudover have væsentlig samfundsmæssig betydning. Bredt forstået vil projektet have "væsentlig samfundsmæssig betydning", når det klart og positivt gavner samfundet. Det vil typisk være tilfældet, når projektet har til formål:

- at forbedre samfundets sundhed og trivsel,
- at forbedre den finansielle eller økonomiske situation for samfundet som helhed,
- at bidrage til viden på et givent område, eller
- at bidrage til udviklingen af mere effektive produkter, ydelser og processer for samfundet.

For at en undersøgelse kan siges at have væsentlig samfundsmæssig interesse, er det således ikke tilstrækkeligt, at undersøgelsen alene tilgodeser jeres (myndighedens) egen interesse. Det betyder ikke, at I ikke (også) selv kan have en interesse i udviklingen af den pågældende løsning. Det er dog en betingelse, at I også kan pege på noget, som gavner samfundet mere bredt, og udviklingsprojektets samfundsmæssige betydning må ikke være et underordnet eller perifert hensyn i forhold til jeres det primære hensyn, som projektet skal tilgodese.

Eksempel 7

En kommune ønsker at udvikle et beslutningsstøtteværktøj, der skal understøtte kommunens vurdering af underretning om børn og unges mistrivsel. Løsningen skal tilvejebringe viden om, hvilke forhold der kan føre til eller bidrage til, at børn og unge

28 Kravet om *nødvendighed* i databeskyttelseslovens § 10 vil efter Datatilsynets opfattelse i praksis have en begrænset selvstændig betydning i forhold til de eksisterende krav, der følger af forordningens artikel 5, stk. 1, litra b og litra c om saglighed og proportionalitet.

mistrives. Løsningen skal understøtte socialrådgivernes sagsbehandling ved vurdering af underretninger om mistrivsel.

Løsningen skal udvikles på historiske oplysninger, der fremgår af tidligere underretninger, som kommunen har modtaget. Det omfatter bl.a. oplysninger om underretningsårsager, der kan være f.eks. misbrug hos barnet, kriminalitet, seksuelt krænkende adfærd mv.

Udvikling af AI-løsningen vil dels indebære, at kommunen opnår ny viden om, hvilke konkrete årsager eller forhold der fører til eller har indvirkning på eventuel mistrivsel hos børn og unge. Derudover har udvikling af løsningen en væsentlig samfundsmæssig betydning, idet udvikling af løsningen skal bidrage til at sikre børn og unges trivsel og velvære på tværs af kommunen.

Udvikling af løsningen opfylder efter Datatilsynets opfattelse kravene for at bruge databeskyttelseslovens § 10. Det ændrer ikke herved, at kommunen samtidig varetager et hensyn til mere effektiv sagsbehandling af underretninger om mulig mistrivsel, da det primære hensyn er at tilvejebringe ny viden om risikomomenter for mistrivsel samt at sikre børn og unges ve og vel.

Drift af løsningen forudsætter imidlertid fortsat, at kommunen identificerer et passende retsgrundlag, der ikke kan være databeskyttelseslovens § 10.

Eksempel 8

En myndighed har til opgave at behandle ansøgninger om støtte til handicapvenlige ombygninger. Nogle ansøgninger er særligt tidskrævende og vanskelige at sagsbehandle. Det skyldes bl.a., at borgerne ofte undlader at sende de nødvendige dokumenter. Myndigheden ønsker derfor at udvikle en AI-løsning, som skal reducere sagsbehandlingstiden for netop de mest tidskrævende opgaver. Samtidig opnår myndigheden mere viden om, hvilke dokumenter der typisk mangler i de pågældende sager, og kan på baggrund af det lave bedre vejledning om området på myndighedens hjemmeside.

Udviklingen af AI-løsningen skal ske ved træning på historiske tidskrævende sager, som indeholder en lang række personoplysninger om borgere, herunder helbredsoplysninger. Myndigheden vurderer ved at inddrage de ovennævnte momenter, at udvikling af modellen sker i videnskabeligt øjemed.

Det primære hensyn, som myndigheden vil tilgodese med udviklingen af AI-løsningen er imidlertid at bidrage til en hurtigere sagsbehandling. Det andet hensyn – opnåelsen af øget viden om hvilke dokumenter, der sædvanligvis mangler i borgernes ansøgninger – er perifært i forhold til myndighedens primære hensyn, ligesom den nye viden, der tilvejebringes ved udvikling af løsningen, er snæver og navnlig relevant for myndigheden selv.

Efter Datatilsynets opfattelse kan udvikling af løsningen ikke siges at ske i videnskabeligt eller statistisk øjemed. Det skyldes, at effektivisering af myndighedens sagsbehandling ikke kan siges at tilvejebringe ny viden på den måde, der er karakteristisk for videnskabelig eller statistisk forskning.

Når I som myndighed vurderer, om jeres udviklingsprojekt har væsentlig samfundsmæssig betydning, kan I tage udgangspunkt i, hvor stor en del af samfundet projektet vil gavne og hvor meget. Det vil sige, at den samfundsmæssige betydning kan anskues både i sin bredde og sin dybde.

Hvis projektet kun berører en mindre gruppe af personer og kun berører disse personer i begrænset omfang, vil I ikke kunne anvende databeskyttelseslovens § 10. Det skyldes, at projektet i så fald sandsynligvis ikke har væsentlig samfundsmæssig betydning.

Hvis projektet kun gavner en mindre gruppe af personer, men er af væsentlig betydning for de pågældende personer, idet der eksempelvis forskes i bedre diagnosticering af en sjælden og alvorlig sygdom, vil projektet sandsynligvis have væsentlig samfundsmæssig betydning. Betingelsen kan også være opfyldt, hvor projektet berører hele samfundet, men kun i beskeden grad gavner de berørte personer.

Opgaver, der varetages i den offentlige sektor, eksempelvis af kommuner eller regioner, vil i sagens natur ofte have væsentlig samfundsmæssig betydning, da den pågældende myndighed eller institution indtager en rolle, som berører et stort antal mennesker og berører disse betydeligt. Samtidig er eksistensgrundlaget og -berettigelsen for offentlige myndigheder mv., at de varetager en opgave af samfundsmæssig betydning.

Det er dog ikke en selvfølge, at udvikling og træning af AI-løsninger har væsentlig samfundsmæssig betydning, alene fordi udviklingen sker med henblik på anvendelse i den offentlige sektor. Eksempelvis vil forskning i intelligent håndtering af en myndigheds e-mails sjældent have en sådan væsentlig betydning for samfundet i sin bredde eller sin dybde til, at behandlingen vil kunne anses som forskning af væsentlig samfundsmæssig betydning. Det betyder ikke, at udvikling af sådanne løsninger ikke kan ske. Som myndighed skal I blot identificere et andet retsgrundlag end databeskyttelseslovens § 10.

Konsekvenser ved brug af databeskyttelseslovens § 10 til udvikling

Når I har valgt at udvikle og træne jeres AI-løsning på baggrund af databeskyttelseslovens § 10, kan I ikke under udviklings- og træningsfasen agere på baggrund af de anbefalinger, forudsigelser mv., som løsningen genererer, over for de borgere, hvis oplysninger indgår i træning af løsningen.[29] Det gælder, uanset at I undervejs forsøger at indhente borgernes samtykke, idet et sådant skift mellem behandlingsgrundlag ikke er muligt.

Hvis I efterfølgende sætter AI-løsningen i generel drift, f.eks. på baggrund af behandlingsgrundlaget om offentlig myndighedsudøvelse med ophæng i et klart supplerende retsgrundlag, kan I anvende løsningen på tværs af alle borgere. Det betyder, at I også vil kunne træffe konkrete afgørelser eller foranstaltninger, f.eks. om sociale ydelser eller sundhedsfaglig behandling, overfor de borgere, hvis oplysninger indgik i det oprindelige træningsdata.

Formålsbegrænsningen i databeskyttelseslovens § 10 skal derfor forstås således, at I ikke må handle ud fra de anbefalinger, forudsigelser mv., som løsningen generer, mens den er under udvikling. Et hospital må eksempelvis ikke iværksætte patientbehandling på baggrund af forslag til behandling, som løsningen genererer under udvikling. Hospitalet må dog godt iværksætte patientbehandling på grundlag af forslag, der genereres af AI-løsningen ved drift, uanset at forslagene eventuelt angår de samme personer, som indgik i træningsdatasættene.

Eksempel 9

En kommune ønsker at opnå mere viden om borgernes behov for genoptræning og rehabilitering efter længerevarende sygdomsforløb, da kommunen oplever stigende udgifter på dette område. Med henblik på at tilvejebringe denne viden og samtidig give den enkelte borger et større udbytte af sin genoptræning udvikler kommunen i samarbejde med en leverandør en AI-løsning i håbet om at nedbringe udgifterne på området. Løsningen tilrettelægger individuelle træningsforløb for borgerne baseret på en lang række data om bl.a. deres sygdomshistorik. AI-løsningen trænes ved brug af oplysninger fra tidligere sager.

Kommunen behandler oplysninger om borgeren, herunder helbredsoplysninger, med henblik på udførelse af en videnskabelig undersøgelse, idet hensynet bag udviklingen af løsningen er at tilvejebringe ny viden om genoptræning og rehabilitering.

29 Det følger af databeskyttelseslovens § 10, stk. 2.

Kommunen ønsker derudover efterfølgende at sætte den færdigudviklede AI-løsning i drift som led i kommunens myndighedsopgave på området.

Kommunen kan behandle personoplysninger, der findes i de historiske data, på baggrund af databeskyttelseslovens § 10, men kan ikke under udvikling af løsningen tilrettelægge individuelle træningsforløb på baggrund af de forslag, som AI-løsningen genererer.

Når kommunen efterfølgende sætter løsningen i drift, kan kommunen dog godt tilrettelægge individuelle træningsforløb – også for de samme borgere, hvis oplysninger indgik i træningsdatasættet. Forudsætningen for, at kommunen kan sætte løsningen i drift er imidlertid fortsat, at kommunen kan identificere et klart retsgrundlag, f.eks. i serviceloven, for den behandling af personoplysninger, der sker som led i drift af løsningen.

Mellem udvikling og idriftsættelsen af en AI-løsning vil den udviklede løsning ofte blive testet. I vil eksempelvis anvende den udviklede model på en begrænset gruppe af personer i et kontrolleret miljø med henblik på at teste, om modellen har brister eller fejl.

På dette tidspunkt vil behandlingen af personoplysninger i AI-løsningen typisk ske med henblik på at generere forudsigelser, anbefalinger eller lignende om et begrænset antal borgere, som indgår i det datasæt, der anvendes til test. Løsningen vil – på samme måde som hvis løsningen var i drift – generere et output, f.eks. en forudsigelse om risikoen for, at en borger skal langtidsindlægges. Dette output kan indgå i jeres arbejde med at teste, om løsningen er fejlfri, f.eks. ved at foretage en menneskelig (i dette tilfælde lægelig) vurdering af samme borger med henblik på at efterprøve den genererede forudsigelse. I kan imidlertid ikke iværksætte sundhedsbehandlingen over for den pågældende borger baseret på output fra testfasen.

I det omfang udvikling af en AI-løsning helt eller delvist kan betragtes at ske i statistisk eller videnskabeligt øjemed, vil testen af sådanne løsninger kunne anses som en del af det statistiske eller videnskabelige formål. Det betyder, at behandlingen af personoplysninger i denne fase også kan ske på baggrund af databeskyttelseslovens § 10. Det skyldes, at formålet med en sådan test af løsningen typisk er at efterprøve rigtigheden af det output, som løsningen genererer, og afprøve løsningens pålidelighed. Desuden vil test ofte ske i et kontrolleret miljø, og løsningen kan dermed ikke anses for at være taget i drift.

En manglende mulighed for at teste AI-løsninger på baggrund af lovens § 10 ville i mange tilfælde afskære muligheden for at foretage en fyldestgørende vurdering af, om den udviklede løsning fungerer efter hensigten. En test af løsningen kan således være essentiel for at opnå det statistiske eller videnskabelige formål med udviklingen og træningen af AI-løsningen.

Det er imidlertid vigtigt, at I er opmærksomme på, at databeskyttelseslovens § 10 ikke kan udstrækkes til at omfatte anvendelse af AI-løsningen efter testfasen som et led i jeres daglige drift.

Selvom det kan forekomme oplagt at udvikle og træne en AI-løsning på baggrund af databeskyttelseslovens § 10, som fastsætter en række mere lempelige vilkår for behandlingen af personoplysninger, er det de faktiske omstændigheder ved udviklingsprojektet, der fastlægger, om bestemmelsen kan bruges. Bestemmelsen kan således ikke bruges frit, hvis de faktiske omstændigheder ikke indikerer, at behandlingen af personoplysninger reelt sker alene i videnskabeligt eller statistisk øjemed.

Det bemærkes desuden, at drift af løsningen – uanset om udvikling og træning af AI-løsningen er sket på baggrund af databeskyttelseslovens § 10 – forudsætter et særskilt retsgrundlag. I bør derfor allerede i forbindelse med designfasen tage stilling til, om der findes et relevant retsgrundlag til jeres behandling af personoplysninger, når løsningen sættes i drift. Datatilsynet udelukker ikke, at der kan være tilfælde, hvor drift af en AI-løsningen også sker i et statistisk eller videnskabeligt øjemed. I disse tilfælde kan databeskyttelseslovens § 10 også benyttes til drift af den pågældende løsning, men det må antages at have undtagelsens karakter, at det vil være tilfældet.

4.2 Oplysningspligt

Når I indsamler oplysninger hos borgerne eller hos andre, skal I som det klare udgangspunkt oplyse borgerne om, at I behandler deres oplysninger og hvorfor. Det gælder også, når I indsamler oplysninger til brug for udvikling af en AI-løsning.

I kan læse mere om, hvilken information I skal give borgerne mv. i afsnit 3 om oplysningspligten i Datatilsynets generelle vejledning om de registreredes rettigheder.[30]

Hvis I overvejer at udvikle AI-løsninger ved brug af egne, eksisterende data, f.eks. historiske sager, skal I være opmærksomme på jeres pligt til at oplyse borgerne om det. Det skyldes kravet om, at borgerne skal informeres på ny, når oplysningerne skal bruges til andre formål end det, som de oprindeligt blev indsamlet til. Som beskrevet ovenfor i afsnit 3.1. anses udvikling af en AI-løsning for at være et nyt formål i forhold til eksempelvis sagsbehandling i forvaltningen.

Kravene til, hvilken information I skal give borgerne, afhænger af situationen. Der sondres mellem den situation, hvor I har indsamlet oplysningerne hos borgerne, f.eks. hvis en borger har sendt en ansøgning til jer, og den situation, hvor I ikke har indsamlet oplysningerne hos borgerne, f.eks. hvis I har modtaget oplysninger fra en anden myndighed til brug for jeres sagsbehandling.[31]

Hvis I ønsker at genanvende data, som I allerede ligger inde med, skal I sørge for at informere borgerne om den påtænkte anvendelse, inden det sker.

Eksempel 10

En kommune ønsker at udvikle en AI-løsning til at fremsøge tidligere ansøgningssager om kropsbårne hjælpemidler. Løsningen skal udvikles ved brug af gamle ansøgningssager. Det drejer sig derfor om oplysninger, som kommunen har modtaget fra borgerne selv.

Kommunen har ikke tidligere oplyst borgerne om, f.eks. i forbindelse med ansøgningen, at oplysningerne ville blive brugt til at udvikle en AI-løsning.

Kommunen skal derfor give borgerne en række informationer om, at deres oplysninger vil blive (gen)brugt til dette nye formål. Det følger af forordningens artikel 13.

Hvis I ønsker at bruge data fra andre myndigheder, skal I som det klare udgangspunkt også sørge for at oplyse borgerne om, at I modtager disse datasæt, og hvad I vil bruge dem til.

Eksempel 11

En kommune ønsker at udvikle en AI-løsning til at understøtte visitation af genoptræningsplaner, som kommunen er forpligtet til at tilbyde efter sundhedsloven. Løsningen skal udvikles ved brug af tidligere genoptræningsplaner. Oplysningerne stammer oprindeligt fra regionerne, som har indsamlet oplysningerne som led i patientbehandling.

Hverken regionerne eller kommunen har tidligere oplyst borgerne om, at oplysningerne vil blive brugt til at udvikle en AI-løsning.

30 Datatilsynets vejledning om de registreredes rettigheder, juli 2018.

31 Hvis I har indsamlet oplysningerne direkte hos borgerne, findes kravene i databeskyttelsesforordningens artikel 13. Hvis I derimod har modtaget oplysningerne andetsteds fra, findes kravene i artikel 14.

Kommunen skal derfor give borgerne en række informationer om, at deres oplysninger vil blive (gen)brugt til dette formål. Det følger af forordningens artikel 14.[32]

I har dog ikke pligt til at oplyse borgerne om, at I bruger oplysningerne til et nyt formål, hvis det udtrykkeligt fremgår af lovgivningen, at I foretager denne behandling af oplysningerne.

Hvis I viderebehandler oplysningerne på baggrund af en bekendtgørelse udstedt i medfør af databeskyttelseslovens § 5, stk. 3, skal I ikke oplyse borgerne om viderebehandlingen. Det gælder dog ikke, hvis det nye formål er sammenstilling eller samkøring af oplysninger i kontroløjemed.[33]

Økonomisk støtte til modtagere af ældrecheck og engangsbeløb til uddannelsessøgende – undtagelse fra oplysningspligten

Det fremgår af lov om en ekstra økonomisk støtte til modtagere af ældrecheck og engangsbeløb til uddannelsessøgende, der modtager stipendium som tillæg på grund af en funktionsnedsættelse eller som enlige forsørgere § 6, stk. 1, at Uddannelses- og Forskningsstyrelsen videregiver personnumre på uddannelsessøgende til Arbejdsmarkedets Tillægspension til brug for udbetaling af engangsvederlag.

Bestemmelsen er et eksempel på, at en myndighed kan undlade at opfylde oplysningspligten i forbindelse med viderebehandling – videregivelse af personoplysninger til en anden myndighed – i medfør af databeskyttelsesforordningens artikel 14, stk. 5, litra c. Det skyldes, at Uddannelses- og Forskningsstyrelsen er underlagt en pligt til at videregive de pågældende oplysninger til Arbejdsmarkedets Tillægspension, og dette fremgår tydeligt at bestemmelsen.

Kommunalbestyrelsers videregivelse af oplysninger fra CPR til private – ingen undtagelse fra oplysningspligten

Det følger af CPR-lovens § 43, stk. 1, at kommunalbestyrelser kan videregive beskyttede navne og adresser i CPR til private, der har en retlig interesse i sådanne oplysninger om en forud identificeret person.

Bestemmelsen er et eksempel på, at en myndighed ikke udtrykkeligt er underlagt en pligt til at videregive oplysninger, men har muligheden for det (jf. "*kan videregive*"). Kommunalbestyrelser vil ikke med henvisning til denne bestemmelse kunne undlade at opfylde deres oplysningspligt efter artikel 14, stk. 5, litra c, da borgerne ikke ud fra bestemmelsen kan se, at deres oplysninger vil blive videregivet.

Der findes en række andre undtagelser til forpligtelsen til at oplyse borgerne om en behandling af deres oplysninger. Det gælder bl.a. hvis borgerne allerede er bekendt med oplysningerne. Om denne undtagelse kan bruges afhænger af, hvilke informationer I har givet borgerne i forbindelse med indsamlingen af deres oplysninger. Hvis borgerne på det tidspunkt, de afgav oplysningerne, ikke blev informeret bl.a. om de formål, oplysningerne skulle bruges til (træning af en AI-løsning til et eller flere formål), kan I ikke benytte undtagelsen, idet borgerne ikke er bekendt med alle de nødvendige oplysninger.

32 Det er Datatilsynets opfattelse, at ingen af undtagelserne i forordningens artikel 14 eller databeskyttelseslovens § 22 er relevante i dette tilfælde.

33 Databeskyttelseslovens § 23.

Derudover kan der være et hensyn til jer som myndighed eller til borgerne selv, som medfører, at borgerne ikke skal oplyses om en behandling.

Hvis I ikke har indsamlet oplysningerne hos borgerne, er I desuden ikke forpligtede til at oplyse dem om behandlingen af deres oplysninger, hvis det er umuligt eller vil kræve en uforholdsmæssigt stor indsats. Hvis det er tilfældet, skal I dog træffe andre passende foranstaltninger for at beskytte borgernes rettigheder, f.eks. ved at offentliggøre informationerne på jeres hjemmeside.

I kan læse mere om undtagelserne til oplysningspligten i afsnit 3.4.3 og 3.5.3 i Datatilsynets vejledning om de registreredes rettigheder.[34]

Eksempel 12

En forsker på et universitet ønsker at udvikle en AI-løsning, der skal identificere mulige risikofaktorer for anbringelse af børn og unge. Løsningen skal udvikles ved brug af oplysninger fra en myndigheds register, som indeholder oplysninger om anbragte børn og unge fra de sidste 50 år.

Forskeren konstaterer dog, at en række af kontaktoplysningerne i registret er forældede. Idet forskeren ikke har mulighed for at finde borgernes kontaktoplysninger på anden vis, kan forskeren ikke oplyse borgerne om behandlingen af deres oplysninger.

Det er Datatilsynets opfattelse, at universitetet i dette tilfælde kan undlade at opfylde oplysningspligten, da det er umuligt eller i hvert fald vil kræve en uforholdsmæssigt stor indsats. Som en kompenserende foranstaltning vælger forskeren at oprette en hjemmeside, hvor oplysninger om forskningsprojektet kan findes.[35]

I skal også være opmærksomme på, at I som dataansvarlige ikke er forpligtet til at indhente flere oplysninger om borgerne alene for at kunne at opfylde oplysningspligten. Det vil i eksemplet indebære, at universitetet ikke er forpligtet til at samkøre de oplysninger, som universitetet er i besiddelse af, med oplysninger fra CPR-registeret alene med det formål at finde eventuelle kontaktoplysninger for at kunne opfylde oplysningspligten, jf. databeskyttelsesforordningens artikel 11.

34 Se nærmere i Datatilsynets vejledning om de registreredes rettigheder, juli 2018, samt Artikel 29-gruppens retningslinjer for gennemsigtighed i henhold til forordning 2016/679, WP260.

35 Forpligtelsen til at træffe passende foranstaltninger i tilfælde, hvor der viser sig umuligt eller vil kræve en uforholdsmæssig stor indsats at oplyse borgerne om behandling af deres personoplysninger, følger af databeskyttelsesforordningens artikel 14, stk. 5, litra b, 2. led.

5. Driftsfasen

Når en AI-løsning implementeres i myndighedens daglige drift, vil den typisk blive brugt til at løse en konkret opgave i praksis. Det kan være en eksisterende myndighedsopgave, som AI-løsningen skal bidrage til at løse mere effektivt. Det kan også være en helt ny myndighedsopgave, som myndigheden fra begyndelsen vurderer bedst kan løses ved brug af AI. AI-løsninger i den offentlige sektor vil således f.eks. kunne bruges som beslutningsstøtte for sagsbehandlere på beskæftigelsesområdet, træffe afgørelse i enkle ansøgningssager, udvælge virksomheder og borgere til kontrol på skatteområdet, tolke scanningsbilleder på hospitaler, forudsige patienters risiko for komplikationer som følge af et kirurgisk indgreb og meget andet. Fælles for disse formål er, at anvendelsen af sådanne løsninger i den offentlige sektor skal understøtte myndighedsudøvelsen.

5.1 Formål

Mens behandlingen af personoplysninger til brug for udvikling af en AI-løsning anses som et særskilt formål, er drift af en AI-løsning er dog nærmere knyttet til udførelsen af jeres myndighedsopgaver. Derfor vil drift af AI-løsningen ofte ikke anses som et særskilt formål, men blot understøtte den eksisterende myndighedsopgave. Der kan dog være tilfælde, hvor drift af løsningen sker som led i et nyt formål. Det kan f.eks. være tilfældet, hvor myndigheden skal varetage en ny opgave, som myndigheden ikke tidligere har varetaget, og som fra start skal ske ved brug af en AI-løsning.

Under alle omstændigheder vil brug af AI-løsninger typisk aktualisere (ofte høje) risici for borgerne, f.eks. hvis AI-løsningen i drift har til formål at producere forudsigelser, anbefalinger mv. om borgeren, som myndigheden vil handle ud fra. Dette vil udgøre et indgreb i borgerens konkrete forhold, som efter omstændighederne kan være større eller mindre.

Der vil derfor være behov for, at I vurderer, om jeres eventuelle behandlingsgrundlag er tilstrækkelig klart og tydeligt til, at I kan sætte løsningen i drift. Nogle behandlingsgrundlag vil desuden ikke være tilgængelige for jer til brug for drift af AI-løsningen, såsom databeskyttelseslovens § 10, jf. nærmere herom ovenfor afsnit 4.1.2. I så fald vil I være nødt til at identificere et andet behandlingsgrundlag, medmindre AI-løsningen anvendes som led i et statistisk eller videnskabeligt øjemed.

5.2 Relevante behandlingsgrundlag

Når AI-løsningen er færdigudviklet og -trænet, og I ønsker at sætte løsningen i drift, skal I have et behandlingsgrundlag for den behandling af personoplysninger, som vil ske ved drift af løsningen. Hvis der er tale om en dynamisk model, der også i driftsfasen kontinuerligt lærer og udvikler sig på grundlag af de data, den behandler, må der identificeres et behandlingsgrundlag til både formålet om udvikling og formålet med at anvende løsningen i drift. Se nærmere herom i afsnit 5.3.

Personoplysninger kan behandles på baggrund af et af flere behandlingsgrundlag, som findes i databeskyttelsesforordningens artikel 6, stk. 1. I praksis vil offentlige myndigheder typisk behandle borgernes personoplysninger, fordi det er nødvendigt for at overholde en retlig forpligtelse,[36] eller med henblik på at udføre en opgave i samfundets interesse eller som led i sin offentlige myndighedsudøvelse.[37] Behandlingen skal i disse tilfælde altid have et såkaldt supplerende retsgrundlag i EU-retten eller dansk ret.

36 Databeskyttelsesforordningens artikel 6, stk. 1, litra c.

37 Databeskyttelsesforordningens artikel 6, stk. 1, litra e.

5.2.1 Retlig forpligtelse

En retlig forpligtelse skal ikke nødvendigvis være en lov, men kan også være regler udstedt i medfør af lov, f.eks. bekendtgørelser og andre administrative forskrifter. Endvidere skal en retlig forpligtelse være tilstrækkelig klar med hensyn til den behandling af personoplysninger, som den kræver. Den retlige forpligtelse skal derfor udtrykkeligt henvise til karakteren af og genstanden for behandlingen, og I må som myndighed ikke have unødige skønsbeføjelser med hensyn til, hvordan den retlige forpligtelse skal overholdes.[38] Hvis I som myndighed baserer jeres behandling af oplysninger i en AI-løsning på en retlig forpligtelse, skal det klart fremgå af lovgivningen, at I er forpligtet til at behandle de pågældende oplysninger, og I må kun behandle oplysningerne i det omfang, det er nødvendigt for at overholde den specifikke retlige forpligtelse.

Indberetning af lønindkomst – retlig forpligtelse

Skatteindberetningslovens § 1 fastsætter, at alle arbejdsgivere hver måned skal indberette deres ansattes indkomst til indkomstregistret. Af bestemmelsens stk. 2-4 fremgår de specifikke oplysninger i form af indkomsttyper, der skal oplyses om i indberetningen, herunder løn, gratiale, godtgørelse for udgifter påført i forbindelse med arbejdet eller anvendt til kurser og uddannelse mv.

Bestemmelsen er et eksempel på en klar retlig forpligtelse til at behandle, her indberette, personoplysninger.

5.2.2 Opgave i samfundets interesse eller offentlig myndighedsudøvelse

Hvis lovgrundlaget ikke præcist angiver, at I skal behandle specifikke personoplysninger med henblik på at udvikle eller bruge en eller flere AI-løsning(er), vil det som udgangspunkt være udførelse af en opgave i samfundets interesse eller offentlig myndighedsudøvelse, som udgør jeres behandlingsgrundlag. Det skal dog fortsat fremgå af lovgivningen, at der er tale om en opgave, som I er forpligtet eller berettiget til at udføre. Det kan f.eks. være løsningen af opgaver inden for det sociale område, som I skal varetage i henhold til servicelovens bestemmelser.

Støtte til hjælpemidler – pålagt myndighedsopgave

Efter servicelovens § 112 skal kommuner i visse tilfælde yde støtte til hjælpemidler til personer med varigt nedsat fysisk eller psykisk funktionsevne.

Bestemmelsen er et eksempel på en opgave, som kommuner er forpligtet til at udføre.

For at behandling kan anses for nødvendig af hensyn til udførelsen af en opgave i samfundets interesse, skal opgaven være af almen interesse og dermed af betydning for en bredere kreds af personer. Dette vil f.eks. være tilfældet med behandling i historisk, statistisk eller videnskabeligt øjemed. Der kan være tale om behandling til varetagelse af en opgave i samfundets interesse, uanset at der samtidig forfølges eksempelvis et kommercielt formål, og generelt må begrebet forstås bredt, når behandlingen foretages af offentlige myndigheder.

For at personoplysninger kan behandles med henvisning til en retlig forpligtelse eller en opgave i samfundets interesse eller myndighedsudøvelse, skal behandlingen som nævnt være forudsat i EU-retten eller dansk ret.

Der kræves dog ikke nødvendigvis en specifik lov for hver behandlingsaktivitet. Det kan være tilstrækkeligt med én lov som grundlag for flere behandlingsaktiviteter, som baseres på en retlig forpligtelse, eller som er nødvendige for at udføre en opgave i samfundets interesse eller

38 Justitsministeriets betænkning nr. 1565/2017, s. 117f. og s. 130.

som en del af offentlig myndighedsudøvelse. Retsgrundlaget bør endvidere være klart og præcist, og anvendelsen af reglerne bør være forudsigelig for de borgere, der omfattes af reglerne.[39]

Kravene til klarheden af det retsgrundlag, som skal danne baggrund for jeres behandling af personoplysninger ved drift af en AI-løsning, afhænger af, hvor indgribende behandlingen er for borgerne. Efter Datatilsynets opfattelse skal retsgrundlaget vurderes ud fra, hvor direkte og indgribende f.eks. en afgørelse eller aktivitet er for borgerne. Det gælder uanset, om aktiviteten er bebyrdende eller begunstigende. Retsgrundlaget skal stå i rimeligt forhold til det legitime formål, der forfølges, og behandlingen må ikke være mere indgribende end nødvendigt.

Efter Datatilsynets opfattelse stilles der forskellige krav til klarheden af det relevante retsgrundlaget til henholdsvis udvikling og drift af løsningen. Som nævnt ovenfor medfører udvikling af en AI-løsning som altovervejende udgangspunkt ikke direkte konsekvenser for borgerne. Derimod vil en AI-løsning i drift forventeligt generere forudsigelser, anbefalinger mv., som f.eks. skal være beslutningsstøtte for myndighedens sagsbehandlere. Det kan også være, at en AI-løsning skal træffe automatiske afgørelser over for borgerne. Konsekvenserne for borgerne er dermed ofte større, når AI-løsningen er i drift, og der stilles derfor højere krav til klarheden af det retsgrundlag, der danner baggrund for at anvende løsningen i drift.

I vurderingen af, om retsgrundlaget, som I har identificeret, er tilstrækkelig klart, bør I inddrage, hvilke oplysninger der behandles og om hvilke personer, herunder f.eks. sårbare borgere. Derudover skal I inddrage, om den pågældende forudsigelse, afgørelse mv., som AI-løsningen genererer, har indvirkning på borgerens økonomiske, uddannelsesmæssige, sociale, sundhedsmæssige eller lignende forhold.[40] Indvirkningen kan være såvel positiv som negativ. Endelig bør I overveje, om den pågældende behandling, herunder den omstændighed at behandlingen sker ved anvendelse af AI, er forudsigelig og gennemsigtig for borgeren.

Brug af AI-løsninger kan ikke generelt siges altid at være indgribende for borgeren. Myndigheders borgerrettede brug af sådanne løsninger vil dog i sagens natur typisk have indflydelse på borgernes livssituation. Derfor vil den behandling af personoplysninger, som AI-løsningen foretager, ofte være indgribende. Modsat vil brug af AI-løsninger til mere generelle myndighedsopgaver, der ikke er direkte borgerrettede, anses for at være mindre indgribende.

Datatilsynets praksis (j.nr. 2022-212-3676)

I sin vurdering af kommuners hjemmel til at anvende Asta-værktøjet udtalte Datatilsynet, at kravene, der stilles til klarheden af det nødvendige retsgrundlag, afhænger af, hvor indgribende den pågældende behandling er for den registrerede. Er der tale om en helt harmløs behandling, vil kravene ikke være særlig store. Er der derimod tale om en indgribende behandling, som det var med Asta-værktøjet, stilles der større krav til, hvor klart hjemmelsgrundlaget skal være.

Asta var et værktøj, der havde til formål at foretage en maskinel analyse af, hvad en nyligt ledig dagpengemodtagers risiko var for, at den pågældende persons kontaktforløb med jobcenteret blev langvarigt. Asta-værktøjet estimerede bl.a. dagpengesagens og kontaktforløbets varighed på baggrund af en lang række oplysninger om borgeren.

Det var på den baggrund Datatilsynets opfattelse, at der skulle være hjemmel i dansk ret, for at Asta-værktøjet kunne anvendes af kommunerne, som det f.eks. kendes fra § 8, stk. 2, i lov om en aktiv beskæftigelsesindsats. Denne vurdering var således baseret på beskrivelsen af den behandling af personoplysninger, der ville ske ved brug af Asta-værktøjet.

39 Præambelbetragtning nr. 41 og 45 til databeskyttelsesforordningen.

40 Præambelbetragtning nr. 75 til databeskyttelsesforordningen.

Krav til klarheden af lovgrundlaget

Skærpede krav

Direkte indgreb i borgernes forhold

Ikke ubetydelig omfang af særlige kategorier af oplysninger

Omfatter (næsten) udelukkende sårbare borgere, f.eks. ældre, børn, patienter mv.

Eksempel

En AI-løsning har til formål at foretage en maskinel analyse af, hvad en nyligt ledig dagpengemodtagers risiko er for, at den pågældendes kontaktforløb med jobcenteret blev langvarigt. Værktøjet foretager med andre ord en statistisk baseret analyse af borgeren med henblik på at estimere dagpengesagens og kontaktforløbets varighed på baggrund af en lang række oplysninger om borgeren. Det omfatter oplysninger, der stammer fra borgerens seneste dagpengesager, herunder bl.a. oplysninger om borgerens CV, tidligere kontaktforløb, særlige behov, f.eks. tolkebistand, mv.

Der er her tale om sårbare borgere og en omfattende behandling af personoplysninger vedrørende dem. Behandlingen har indgribende konsekvenser for de pågældende borgere, idet AI-løsningens output indgår i sagsbehandlerens samlede skøn og kan have betydning for borgerens konkrete økonomiske situation.

Almindelige krav

Ingen direkte indgreb i borgernes forhold

Få eller mindre omfang af særlige kategorier af oplysninger

Omfatter få sårbare borgere, f.eks. ældre, børn, patienter mv.

Eksempel

En AI-løsning analyserer kommunens data om affaldssortering, herunder mængden af de forskellige kategorier af affald fra forskellige distrikter i kommunen. Formålet er at tilrettelægge en mere hensigtsmæssig afhentningsordning i kommunen, så skraldespande og containere ikke tømmes oftere end nødvendigt. AI-løsningen justerer løbende forventningerne til affaldsproduktionen baseret på ændringer i indgående data og renovationsselskabet tilpasser sine afhentningsruter på dette grundlag.

Her vil der i mindre omfang blive behandlet personoplysninger om borgerne, da det i tyndt befolkede områder kan være muligt at knytte affaldsdata fra et distrikt til enkeltpersoner. AI-løsningens behandling af personoplysninger kan få konsekvenser for den enkelte borger i form af sjældnere eller hyppigere tømning af vedkommendes skraldespande.

Lempeligere krav

Ingen indgreb i borgernes forhold

Ingen eller få særlige kategorier af personoplysninger

Omfatter ikke sårbare borgere, f.eks. ældre, børn, patienter mv.

Eksempel

En AI-løsning analyserer GPS- og andre kørselsdata fra hjemmeplejens biler med henblik på at opnå en mere effektiv udnyttelse af de forhåndenværende køretøjer, da antallet af plejekrævende borgere i kommunen er stigende.

I denne situation vil der alene blive behandlet personoplysninger om (sårbare) borgere i begrænset omfang i form af deres bopælsadresse og længden af hjemmeplejens besøg, og behandlingen har umiddelbart ikke konsekvenser for de pågældende borgere. Resultatet af behandlingen skal således alene anvendes til at organisere brugen af hjemmeplejens biler, og der tilsigtes ikke ændringer i indholdet af den service, borgerne modtager.

5.2.3 Særligt om samtykke

Et samtykke[41] kan i visse tilfælde udgøre det fornødne retlige grundlag for behandling af personoplysninger. Et samtykke skal dog opfylde en række betingelser for at være gyldigt. For at et samtykke er gyldigt, skal det være *frivilligt, specifikt, informeret* og udtryk for en *utvetydig viljestilkendegivelse*.[42] Det er endvidere en betingelse, at den registrerede er blevet informeret om, at samtykket kan *trækkes tilbage*.[43]

Betingelserne for et gyldigt samtykke kan være vanskelige at opfylde, hvis I som offentlig myndighed ønsker at behandle borgernes oplysninger ved brug af en AI-løsning.

Først og fremmest skyldes det, at der ofte vil være en klar skævhed i forholdet mellem borgeren og jer som myndighed. Hvis behandlingen af oplysninger i den konkrete sag, f.eks. en ansøgning om en ydelse eller en tilladelse, har indflydelse på borgerens livssituation – uanset om det er reelt, eller om borgeren blot opfatter det sådan – vil borgerens samtykke ikke kunne anses for frivilligt.[44]

Frivillighedsbetingelsen vil alene kunne anses for opfyldt i situationer, hvor det ikke har hverken opfattede eller reelle negative konsekvenser for borgeren, hvis vedkommende undlader at give sit samtykke. Dette vil f.eks. kunne være tilfældet, hvor borgeren giver samtykke til at modtage servicebeskeder på e-mail eller SMS om afhentning af storskrald i lokalområdet.

Datatilsynets praksis (j.nr. 2022-212-3676)

Styrelsen for Arbejdsmarked og Rekruttering anmodede i 2022 Datatilsynet om en vurdering af spørgsmålet om kommuners hjemmel til at anvende AI-profileringsværktøjet Asta.

Asta-værktøjet havde til formål at foretage en maskinel analyse af risikoen for, at en nyligt ledig dagpengemodtagers kontaktforløb med jobcenteret blev langvarigt. Med andre ord udarbejdede Asta på grundlag af en række data om borgeren en statistisk forudsigelse af dagpengesagens og kontaktforløbets varighed for den pågældende.

Datatilsynet udtalte i den forbindelse bl.a., at et samtykke efter tilsynets opfattelse sjældent vil kunne anses for frivilligt og dermed udgøre et gyldigt behandlingsgrundlag ved behandling af oplysninger om borgeren i den konkrete kontekst, hvor der var tale om en offentlig myndighed, og hvor den offentlige myndighed havde kontrol over borgerens forsørgelsesgrundlag.

Det gjaldt, selvom det i praksis ville være muligt for borgeren at frasige sig behandlingen, det vil sige undgå profileringen, uden at det havde en negativ indvirkning for den pågældende, f.eks. i form af stop af ydelse. Der ville nemlig være en ikke ubetydelig risiko for, at borgeren – uagtet denne mulighed – ville føle sig presset til at samtykke til behandlingen, f.eks. for at undgå at fremstå besværlig eller lignende.

I skal være opmærksomme på, at myndigheder helt generelt skal have hjemmel i lovgivningen for at udføre deres opgaver. I kan altså ikke bruge et samtykke fra borgeren som behandlingsgrundlag, hvis behandlingen falder uden for rammerne af de opgaver, I som myndighed er blevet pålagt. Dette udelukker dog ikke myndigheden fra at vælge samtykke som behandlingsgrundlag efter databeskyttelsesreglerne i situationer, hvor behandlingen ligger inden for rammerne af myndighedens opgaver. Det kan f.eks. være tilfældet, hvis myndigheden ønsker at

41 Databeskyttelsesforordningens artikel 6, stk. 1, litra a.

42 Databeskyttelsesforordningens artikel 4, nr. 11.

43 Databeskyttelsesforordningens artikel 7, stk. 3.

44 Datatilsynets udtalelse af 5. juli 2022 i sagen med j.nr. 2022-212-3676 (Asta-værktøjet). Se ligeledes Det Europæiske Databeskyttelsesråds retningslinjer nr. 05/2020 om samtykke, s. 8, pkt. 16, samt præambelbetragtning nr. 43 til databeskyttelsesforordningen.

give borgerne reel valgfrihed med hensyn til behandlingen af personoplysninger. Et eksempel kunne være myndighedens tilbud om at benytte en app eller lign.

Eksempel 13

En kommune har udviklet en app, som kan forudsige, hvor der er størst sandsynlighed for at finde en ledig parkeringsplads. Borgere kan dermed minimere den tid, de bruger på at finde parkeringsmuligheder.

Appen viser bl.a. den historiske belægning for hver enkelt gade på det tidspunkt, en bilist kører forbi, samt hvor lang tid det typisk vil tage at finde en parkeringsplads i det pågældende område. Samtidig foreslår appen, hvor der er størst mulighed for at finde en ledig parkeringsplads.

For at appen kan fungere efter hensigten, anmoder kommunen om borgernes samtykke til at indsamle personoplysninger om dem, herunder lokationsdata.

Det er Datatilsynets opfattelse, at kommunen vil kunne behandle borgernes personoplysninger til dette formål på baggrund af deres samtykke. I denne situation er der ingen negative konsekvenser – hverken reelle eller opfattede – for borgerne ved at undlade at give samtykke. Parkeringsappen er alene en service, kommunen tilbyder, og bilister bliver ikke stillet ringere i forhold til kommunen i øvrigt, hvis de ikke gør brug af denne service.

Udover frivillighedsbetingelsen kan de komplicerede processer og den manglende gennemsigtighed, som ofte karakteriserer AI-løsninger, stå i vejen for et gyldigt samtykke. Samtykket skal være specifikt og informeret, og I skal kunne håndtere, at samtykket trækkes tilbage, og stoppe behandlingen af de pågældende oplysninger. Det kan være en udfordring ved komplekse AI-løsninger, hvor oplysningerne behandles på mange forskellige måder. Det er helt afgørende for samtykkets gyldighed, at borgeren forstår, hvad vedkommendes oplysninger skal bruges til, og kan til- og fravælge disse formål. Jo mere, I ønsker at anvende oplysningerne til, desto vanskeligere vil det i sagens natur være at opfylde disse betingelser.

I bør derfor som offentlig myndighed som udgangspunkt behandle borgernes oplysninger ved brug af AI-løsninger på baggrund af et andet retsgrundlag end samtykke. Det gælder også ved behandling af særlige kategorier af oplysninger, som er omtalt nærmere nedenfor.

Det bemærkes i den forbindelse, at offentlige myndigheder i flere tilfælde er underlagt bestemmelser i anden lovgivning, som stiller krav om ”samtykke” fra borgeren. I disse tilfælde skal I være opmærksomme på, at selvom der efter den pågældende lovgivning kræves samtykke fra borgeren til at behandle vedkommendes oplysninger, er der ikke nødvendigvis tale om et samtykke i databeskyttelsesreglernes forstand. Et sådant samtykke vil ofte udgøre en garantiforskrift for borgerne, men vil ikke udgøre grundlaget for selve behandlingen af personoplysninger. Behandlingsgrundlaget vil i disse tilfælde ofte være offentlig myndighedsudøvelse efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, hvor den pågældende lovgivning vil udgøre den relevante supplerende nationale lovgivning.

Eksempelvis udgør et samtykke efter lov om retssikkerhed og administration på det sociale område (retssikkerhedsloven) § 11 a ikke et databeskyttelsesretligt samtykke. Det samtykke, som borgeren kan give efter retssikkerhedslovens § 11 a, har til formål at sikre borgernes rettigheder og indflydelse ved behandling af sager omfattet af loven, men udgør ikke grundlaget for behandlingen af personoplysninger. Behandlingsgrundlaget er derimod offentlig myndighedsudøvelse.

5.3 Monitorering og efterlæring

Når en AI-løsning er taget i brug, skal modellen som tidligere beskrevet løbende overvåges og efter omstændighederne gentrænes for at sikre et fortsat retvisende output.

I en statisk model er driftsfasen tydeligt adskilt fra udviklingsfasen, og når modellen er taget i brug, behandler den kun de personoplysninger, som er nødvendige for driftsformålet. Der vil være behov for jævnlig monitorering for at sikre, at modellen forsat behandler og genererer korrekte personoplysninger, men selve modellen ændrer sig ikke ved brug, og man har derfor fuld kontrol over dens behandling af personoplysninger. Hvis der i forbindelse med monitoreringen findes behov for at gentræne modellen, tages den ud af drift og gentrænes i et lukket testmiljø på udvalgte træningsdata. De to formål om udvikling og drift er således ikke tilstede på samme tid, og man har kun brug for at identificere et behandlingsgrundlag til ét formål ad gangen.

En dynamisk model (gen-)trænes derimod kontinuerligt på de nye data, den behandler, mens den er i brug, og man vil have mindre kontrol med behandlingen af personoplysninger, da selve modellen hele tiden ændrer sig. Dette kræver en mere omfattende monitorering for at undgå, at modellen udvikler sig i en uhensigtsmæssig retning, og man skal have den fornødne hjemmel både til at behandle borgernes oplysninger med henblik på at gentræne og udvikle løsningen og til at behandle deres oplysninger som led i myndighedens drift, da de to formål er til stede samtidigt.

5.4 Oplysningspligt

Når I overvejer at sætte jeres AI-løsning i drift, skal I også være opmærksomme på jeres pligt til at oplyse borgerne om behandlingen af deres oplysninger.

Som beskrevet i afsnit 4.2. vil udvikling af en AI-løsning altid udgøre et særskilt formål, som I skal oplyse borgerne om.

Oftest vil drift af en AI-løsning ikke udgøre et særskilt formål. Det vil som regel være tilfældet, hvor myndigheden ønsker at løse en bestemt opgave, og hvor anvendelsen af AI-løsningen knytter sig til løsningen af denne opgave.

I nogle enkelte tilfælde vil drift af en AI-løsning udgøre et særskilt formål. Det betyder, at I både vil skulle oplyse borgerne om, at deres personoplysninger behandles som led i jeres myndighedsopgave, *og* at I anvender en AI-løsning hertil.

Særligt for de dynamiske AI-løsninger, hvor udvikling og træning også forekommer, mens løsningen er i drift, skal I være opmærksomme på, at udviklingen udgør et særskilt formål, som I skal oplyse borgerne om. Se mere herom i afsnit 4.2.

I kan læse mere om, hvilken information I skal give borgerne mv. henvises i afsnit 3 om oplysningspligten i Datatilsynets generelle vejledning om de registreredes rettigheder.[45]

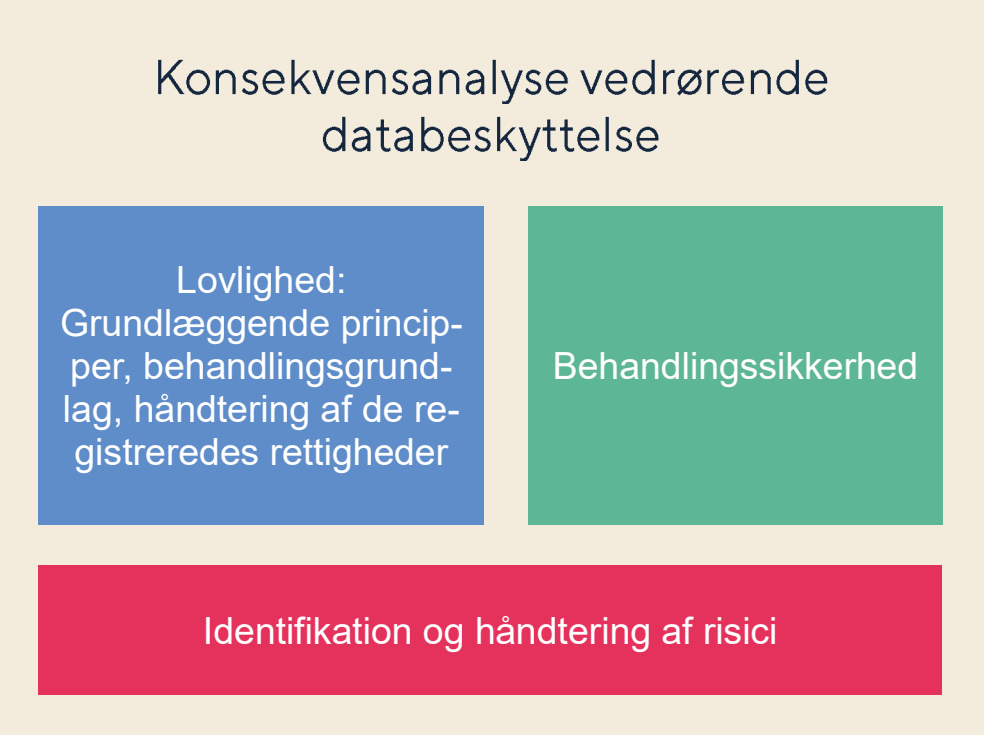
45 Datatilsynets vejledning om de registreredes rettigheder, juni 2018.

6. Konsekvensanalyse

Hvis en behandling af personoplysninger sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal I forud for behandlingen foretage en konsekvensanalyse vedrørende databeskyttelse – en såkaldt *data protection impact assessment (DPIA*).[46] Dette er navnlig relevant, når I ønsker at behandle personoplysninger ved brug af ny teknologi.[47] Det vil efter Datatilsynets opfattelse normalt være tilfældet ved udvikling og brug af AI-løsninger.

En konsekvensanalyse vedrørende databeskyttelse er en proces, der har til formål:

- at beskrive behandlingen af personoplysninger,
- at vurdere behandlingens nødvendighed og proportionalitet, og
- at bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører.



Risikovurdering er også en integreret del af processen med at fastsætte et passende niveau af behandlingssikkerhed, men konsekvensanalysen går et skridt videre end risikovurderingen og indeholder bl.a. også en vurdering af, hvordan de påtænkte behandlingsaktiviteter lever op til de grundlæggende krav om lovlighed.

Konsekvensanalysen indeholder ligeledes en vurdering af risiciene for afvigelser fra den lovlige og tilsigtede behandlingsaktivitet. Derudover omfatter reglerne om konsekvensanalyser en proces for inddragelse af databeskyttelsesrådgiveren, samt eventuel høring af Datatilsynet og/eller borgerne. En konsekvensanalyse har specifikt til formål at sikre en systematisk

46 Databeskyttelsesforordningens artikel 35.

47 Artikel 29-gruppens retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP248, s. 9

undersøgelse af situationer, som kan føre til en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

Under visse betingelser er det et krav at gennemføre en konsekvensanalyse. Betingelserne fremgår af (i) databeskyttelsesforordningen, (ii) Det Europæiske Databeskyttelsesråds retningslinjer om konsekvensanalyser[48], samt (iii) Datatilsynets liste over behandlingsaktiviteter, der altid er underlagt kravet om en konsekvensanalyse[49].

Det er Datatilsynets opfattelse, at behandling af personoplysninger som led i udvikling og/eller drift af AI-løsninger næsten altid vil udløse flere af de kriterier, der er udslagsgivende for, om der skal gennemføres en konsekvensanalyse. Det skyldes:

- at AI anses som såkaldt "ny teknologi", hvilket udgør et af kriterierne i Datatilsynets liste over aktiviteter, der altid er underlagt kravet om en konsekvensanalyse, og
- at udvikling og/eller drift af AI ofte indebærer (i) behandling af særlige kategorier af oplysninger, (ii) behandling af oplysninger om sårbare personer eller (iii) behandling af personoplysninger i stort omfang, hvilket er tre øvrige kriterier der fremgår af Artikel 29-gruppens retningslinjer om konsekvensanalyse.

Konsekvensanalysen bør foretages allerede i planlægnings- og udviklingsfasen af en AI-løsning. I vil dermed så tidligt som muligt i processen blive klar over og kunne adressere eventuelle databeskyttelsesretlige udfordringer forbundet med AI-løsningen.

Konsekvensanalysen vil også gøre jer i stand til at påvise, at I overholder principperne om databeskyttelse gennem design og gennem standardindstillinger. Disse regler indebærer, at I skal implementere tekniske og organisatoriske foranstaltninger, der sikrer at databeskyttelsesreglerne bliver overholdt – og giver derved fornødne garantier for borgernes rettigheder.

Konsekvensanalysen understøtter denne proces og må ses som en løbende forpligtelse, navnlig når behandlingssituationen – som det ofte vil være tilfældet i en AI-løsning – er dynamisk og under konstant forandring.

Princippet om ansvarlighed er en rød tråd gennem hele databeskyttelsesforordningen. Reglerne om databeskyttelse gennem design og gennem standardindstillinger understreger i den forbindelse forpligtelsen til at indtænke databeskyttelsesreglerne allerede fra designfasen og til at overvåge de valgte foranstaltningers effektivitet gennem hele systemets levetid. Kravet om databeskyttelse gennem design og gennem standardindstillinger gælder både i forbindelse med udvikling og design af et system og i forbindelse med dets anvendelse.

AI-systemer, som behandler personoplysninger, bør således fra begyndelsen være designet med henblik på at sikre en effektiv implementering af databeskyttelsesreglerne. Der skal på forhånd være gennemført passende foranstaltninger for at sikre, at forordningens krav og beskyttelseshensyn varetages som en integreret del af hele systemets behandling af personoplysninger. Blandt andet skal det sikres, at træningsdata er repræsentative, at systemets output er rimeligt, at der ikke sker ulovlig forskelsbehandling, og at oplysninger behandles med den fornødne sikkerhed, herunder f.eks. ved brug af pseudonymisering.

Der gælder ingen specifikke formkrav eller en bestemt metodologi for at foretage en konsekvensanalyse. Analysen skal dog som minimum indeholde (i) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, (ii) en vurdering af risiciene for borgernes rettigheder og frihedsrettigheder, samt (iii) de foranstaltninger, der påtænkes for at imødegå disse risici og påvise overholdelse af databeskyttelsesforordningen.[50] Der skal være tale om en egentlig vurdering af risici, der gør det muligt for jer at træffe foranstaltninger for at afhjælpe dem.

48 Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679 (WP248, rev. 01).

49 Listen, der er udarbejdet, jf. databeskyttelsesforordningens artikel 35, stk. 4, kan findes her.

50 Databeskyttelsesforordningens artikel 35, stk. 7, samt præambelbetragtning nr. 84 og 90.

Offentlige myndigheders brug af kunstig intelligens

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk