Rettslige krav for lovlig bruk av personopplysninger til trening av maskinlæringsalgoritmer

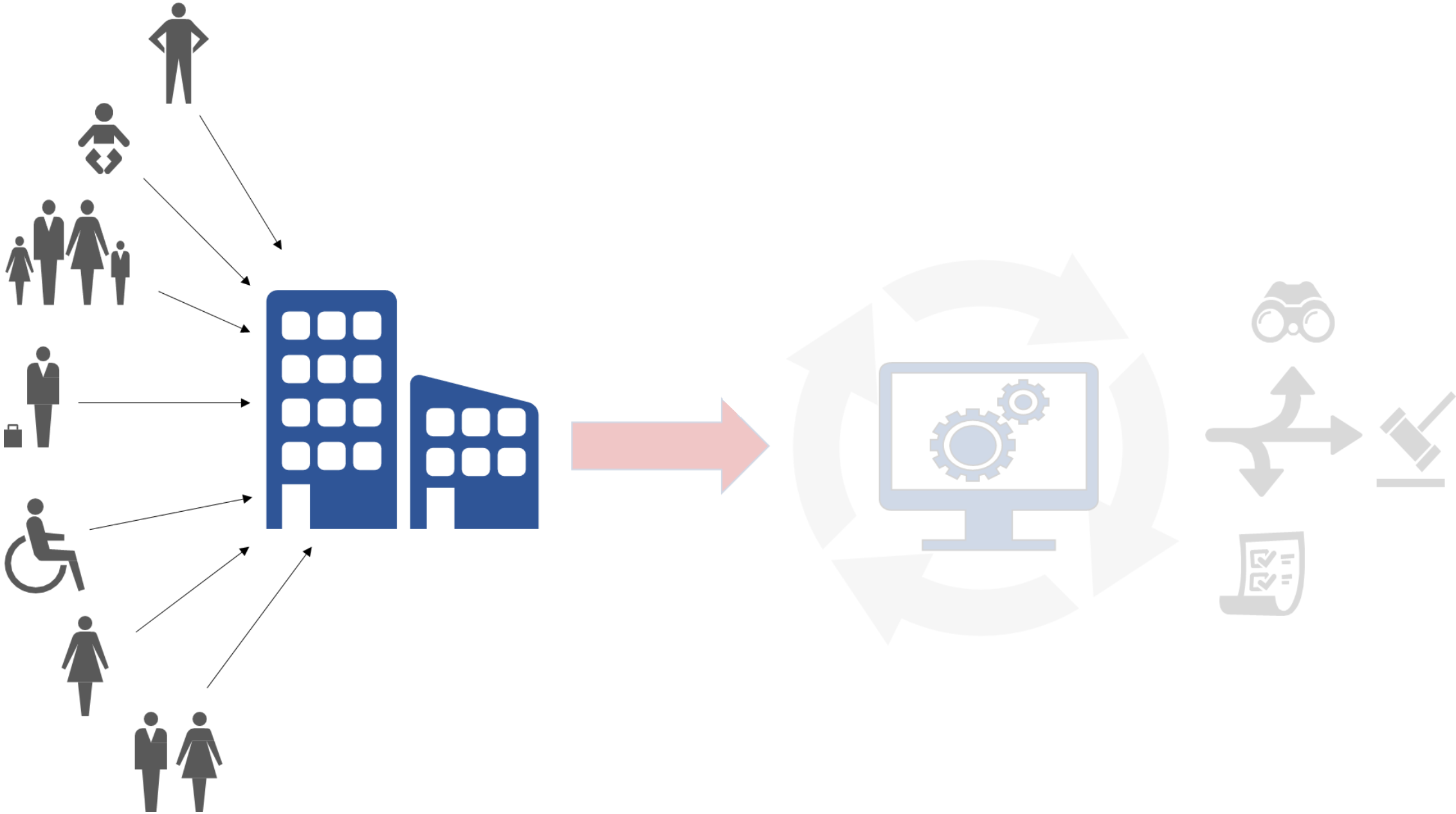
Julie Lossius Husum, KPMG

Seminar om bruk av maskinlæring i offentlig forvaltning – muligheter og problemer, AFIN, 15.09.21

Innsamling av personopplysninger

Trening av ML-algoritmer

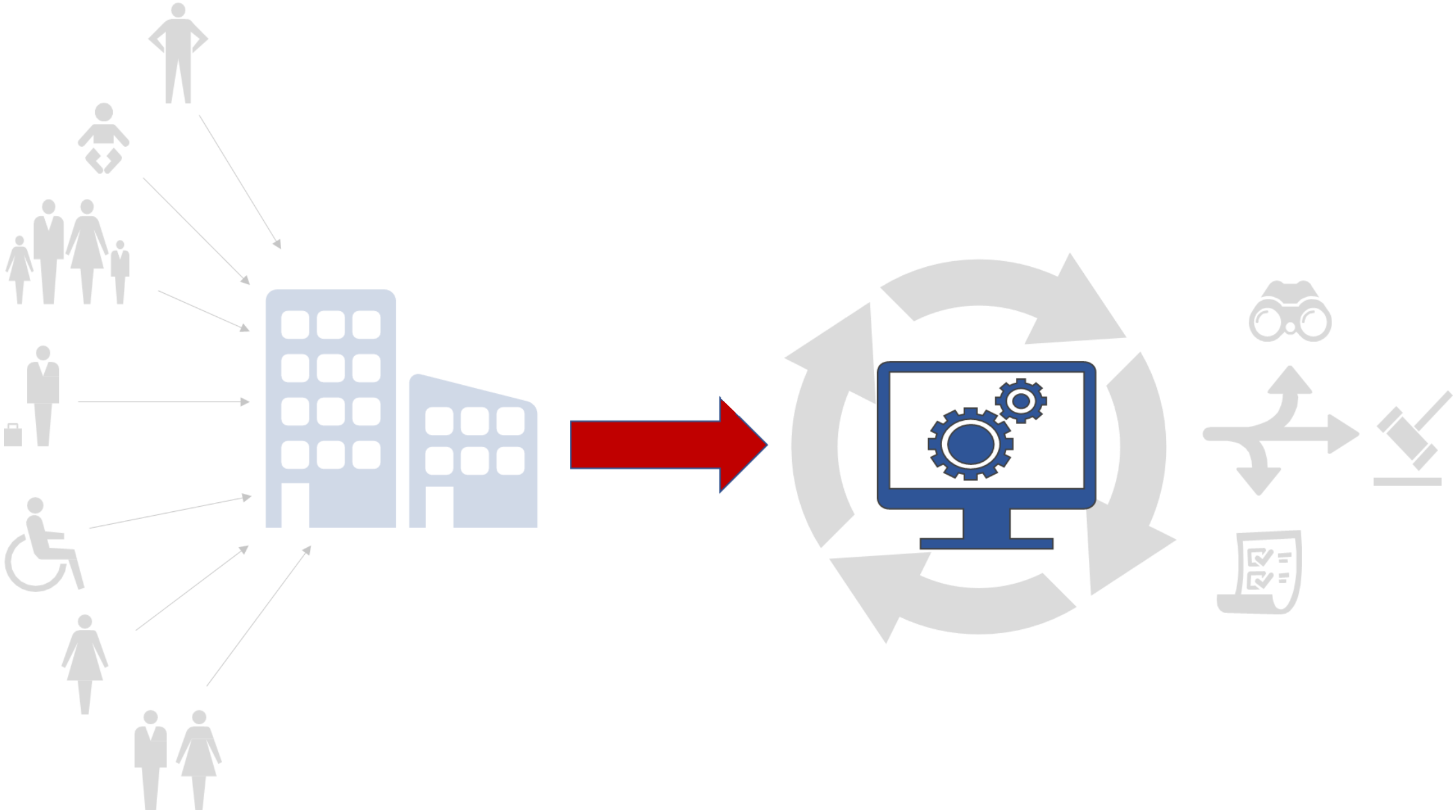
Videre bruk i forvaltningen



Innsamling av personopplysninger

Trening av ML-algoritmer

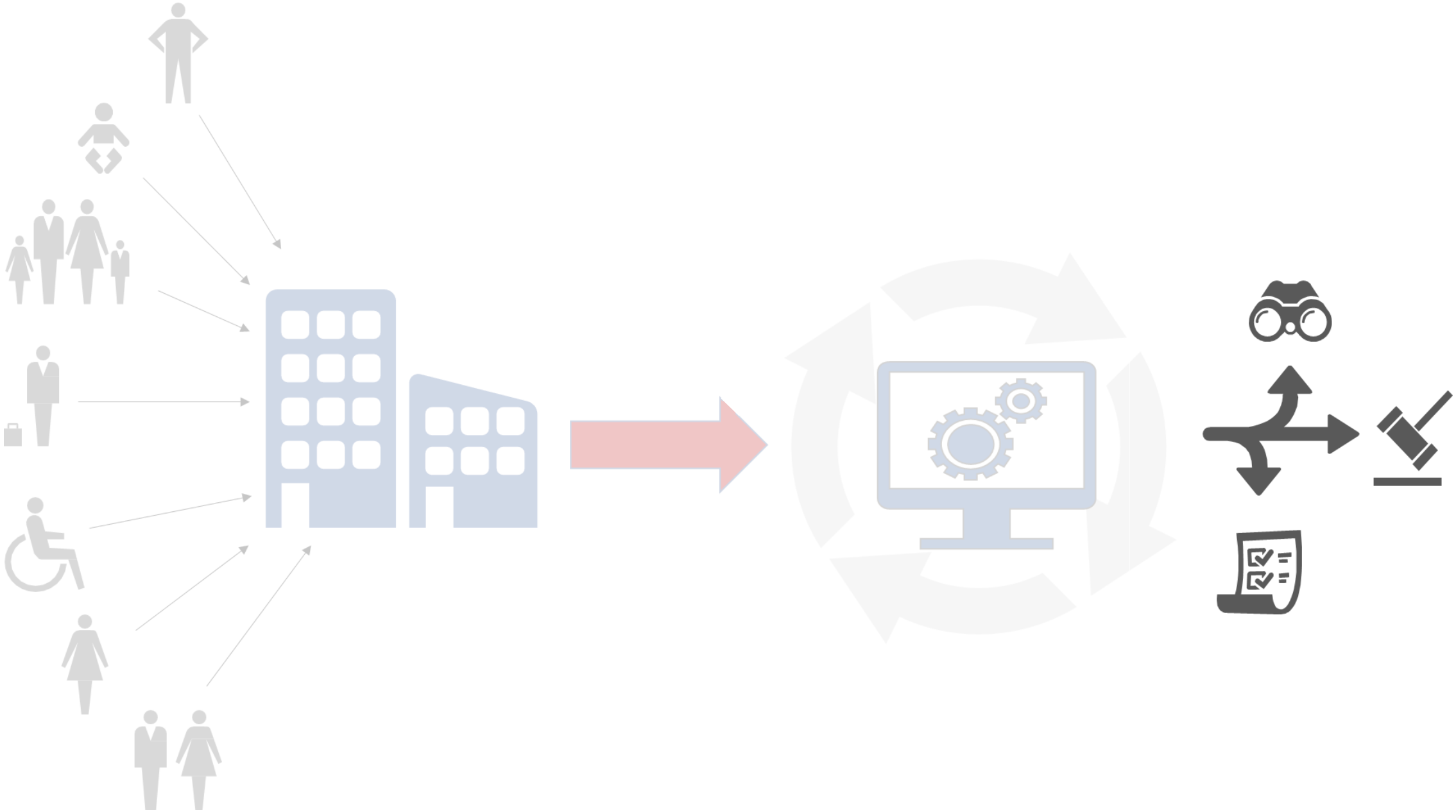
Videre bruk i forvaltningen



Innsamling av personopplysninger

Trening av ML-algoritmer

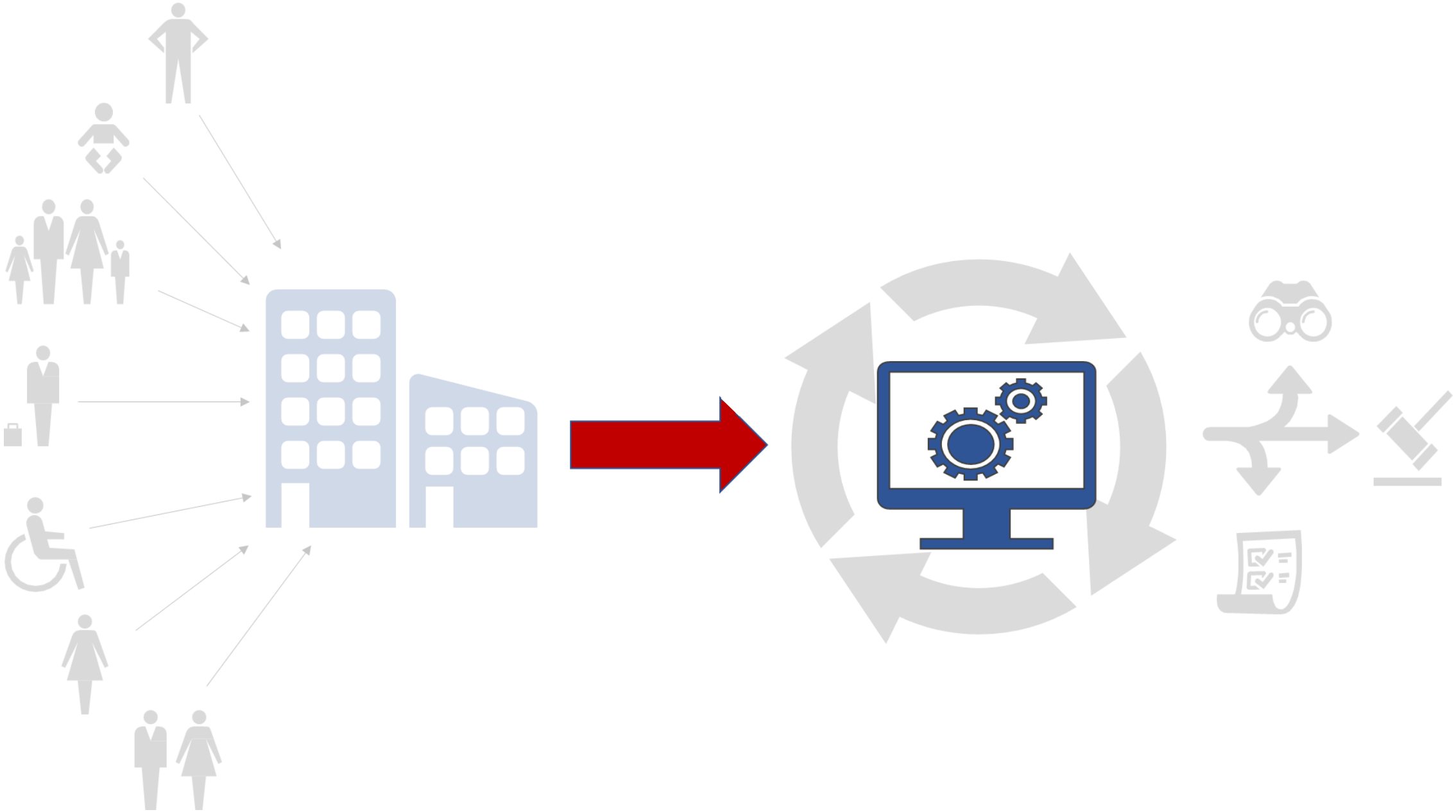
Videre bruk i forvaltningen



Innsamling av personopplysninger

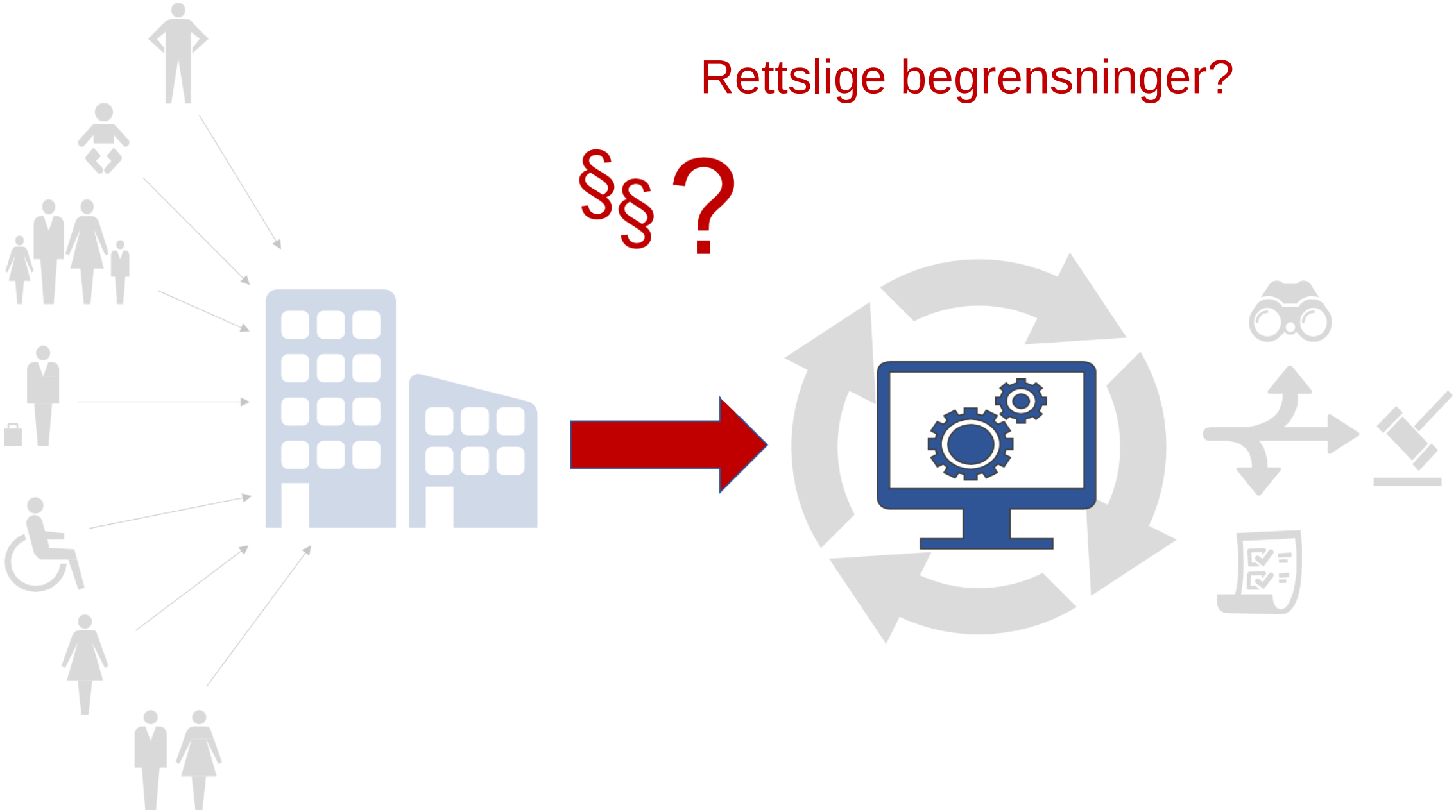
Trening av ML-algoritmer

Videre bruk i forvaltningen



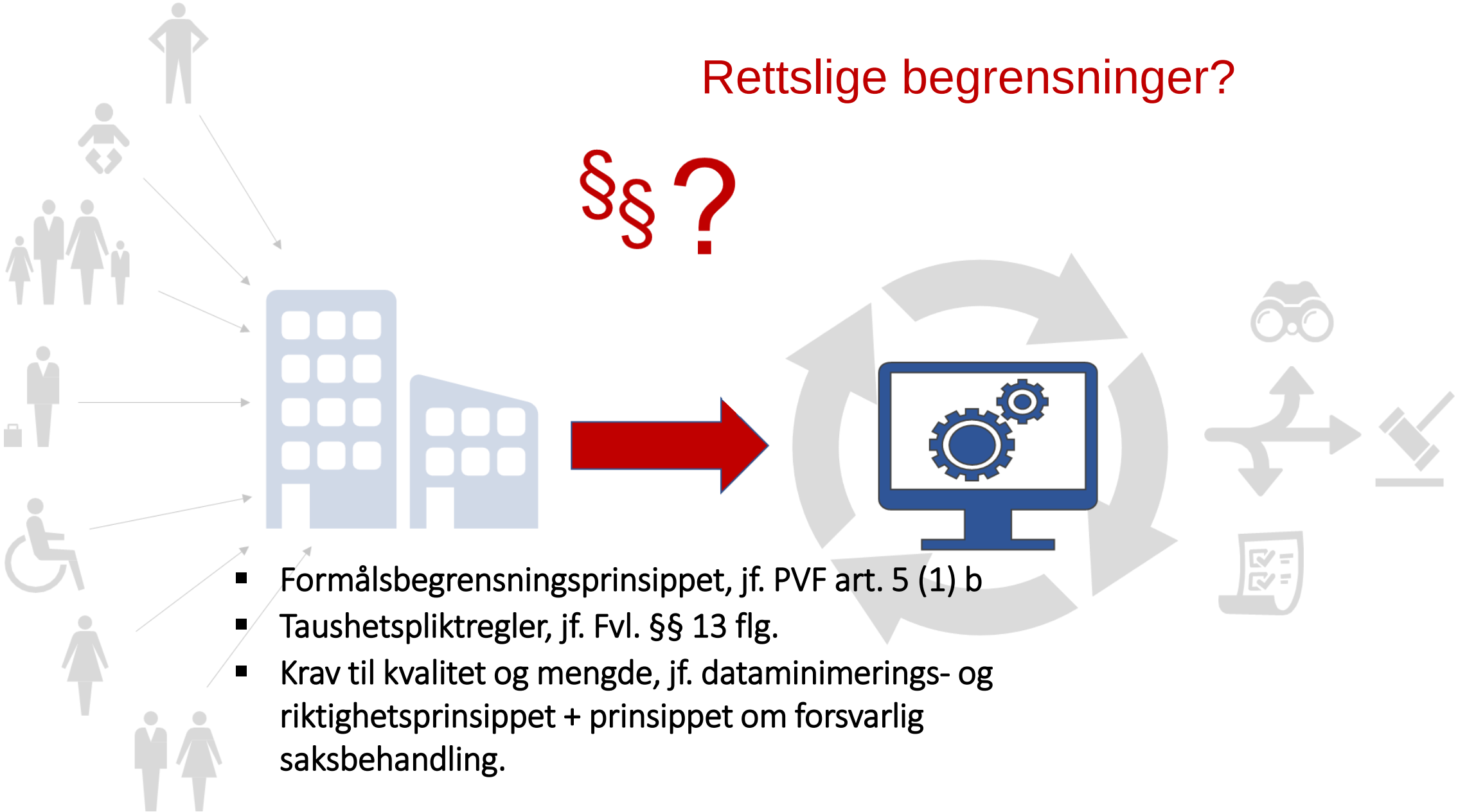
Rettslige begrensninger?

§§ ?



Rettslige begrensninger?

§§ ?



- Formålsbegrensningsprinsippet, jf. PVF art. 5 (1) b
- Taushetspliktregler, jf. Fvl. §§ 13 flg.
- Krav til kvalitet og mengde, jf. dataminimerings- og riktighetsprinsippet + prinsippet om forsvarlig saksbehandling.

Formålsbegrensingsprinsippet, PVF art. 5 (1) b

Formålsbegrensningsprinsippet, jf. PVF art. 5 (1) b

KAPITTEL II Prinsipper

Artikkel 5. ***Prinsipper for behandling av personopplysninger***

1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),

Formålsbegrensningsprinsippet, jf. PVF art. 5 (1) b

Ulike grunnlag for at personopplysninger kan benyttes til å trene ML-algoritmer:

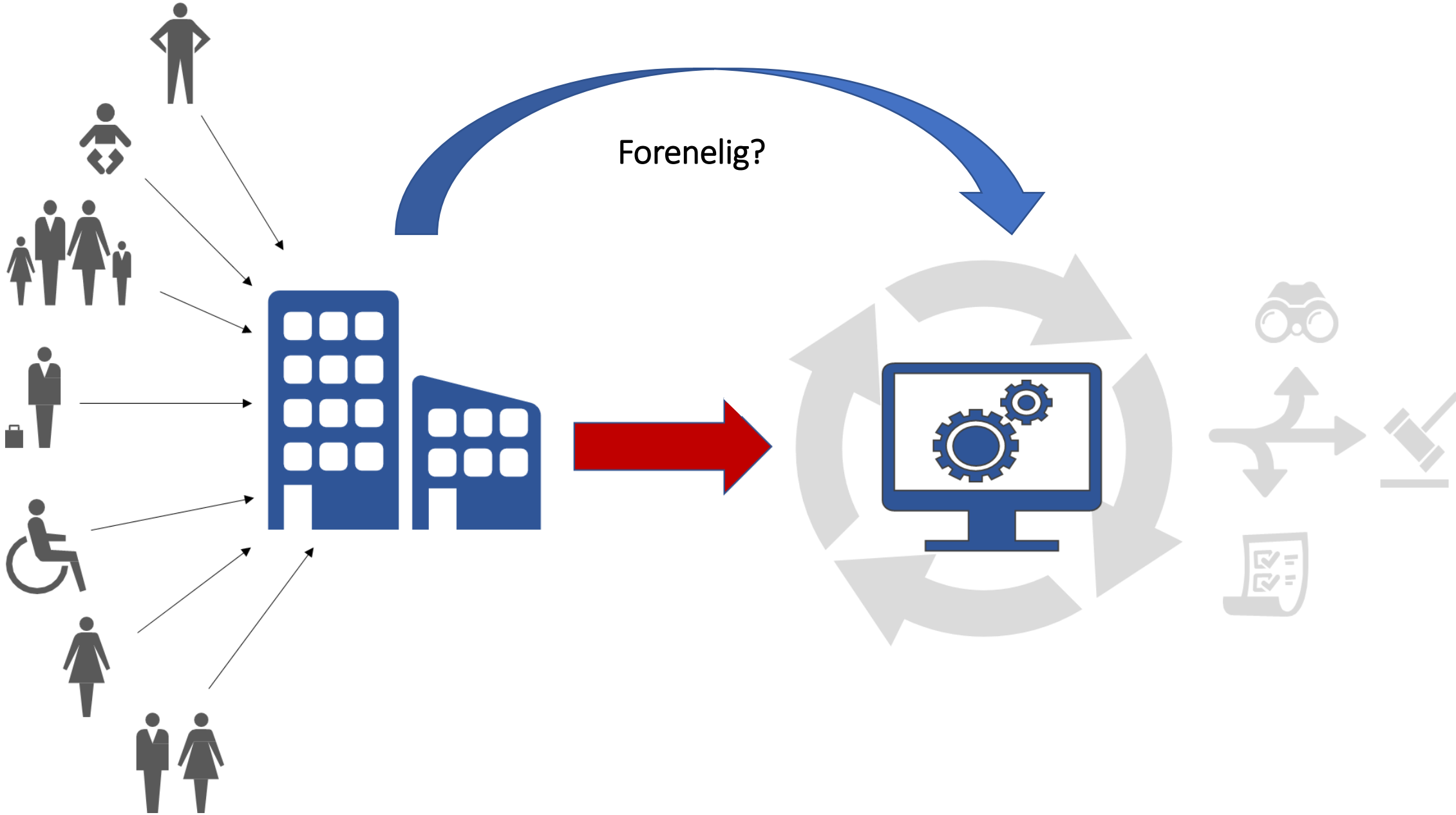
(Lite trolig: Lovlig viderebehandling for arkivformål, vitenskapelig eller historisk forskning eller statistiske formål.)

1. Nytt behandlingsformål må være «forenelig» med opprinnelige formål for innsamlingen.

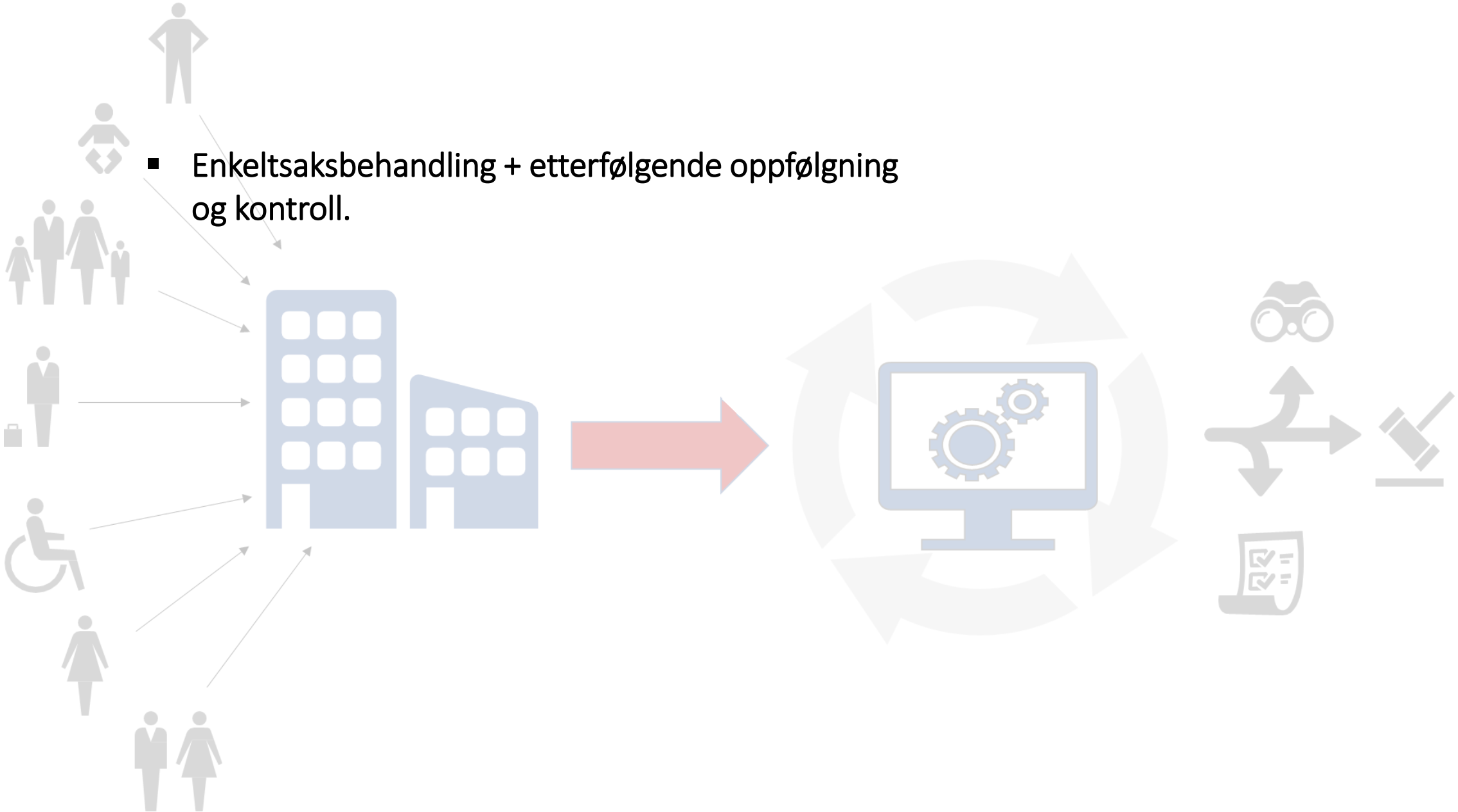
Innsamling av personopplysninger

Trening av ML-algoritmer

Videre bruk i forvaltningen



- Enkeltsaksbehandling + etterfølgende oppfølgning og kontroll.



Formålsbegrensningsprinsippet, jf. PVF art. 5 (1) b

Ulike grunnlag for at personopplysninger kan benyttes til å utvikle maskinlæringsalgoritmer:

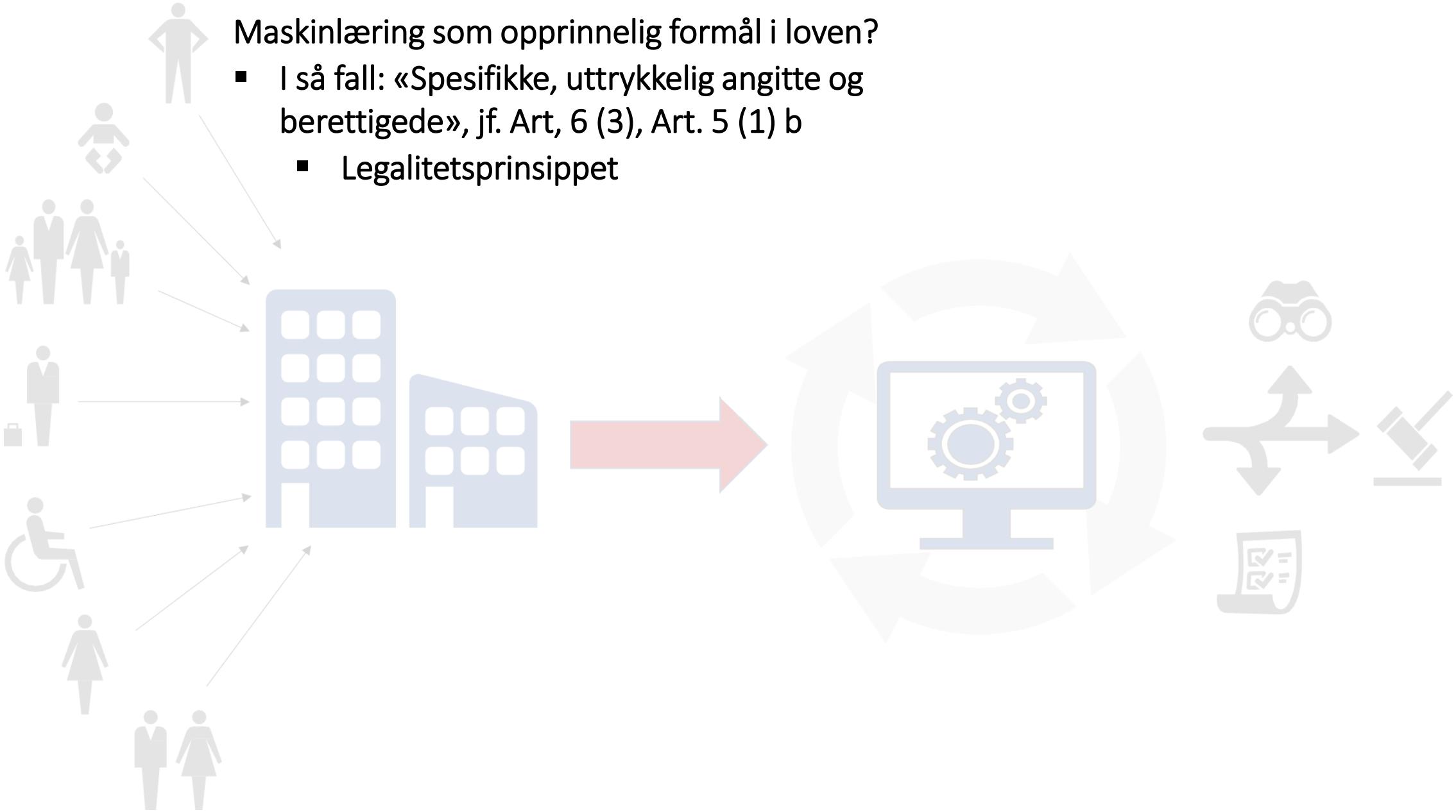
(Sjeldent praktisk: Lovlig viderebehandling for arkivformål, vitenskapelig eller historisk forskning eller statistiske formål)

1. Nytt behandlingsformål må være «forenelig» med opprinnelige formål for innsamlingen

2. Lovlig behandling under primærformålet – viderebehandlingsforbudet aktualiseres ikke

Maskinlæring som opprinnelig formål i loven?

- I så fall: «Spesifikke, uttrykkelig angitte og berettigede», jf. Art, 6 (3), Art. 5 (1) b
  - Legalitetsprinsippet



Trening av ML-algoritmer – forenelig med de opprinnelige formålene for innsamlingen?

For det første: «spesifikke, uttrykkelig angitte og berettigede» må gjelde også formål som angis etter innsamlingen.

Nytt formål forenelig?

- Må vurderes konkret
- Momenter i vurderingen, jf. Art. 6 (4)

a) Forbindelsen mellom formålene

b) Hvilken sammenheng opplysningene er samlet inn

c) Arten av personopplysningene

d) Mulige konsekvenser av den tiltenkte viderebehandlingen for de registrerte

e) Eksistensen av nødvendige garantier

«Forenelig» – kan det sies noe generelt?

Forbindelse mellom opprinnelig formål og trening av ML-algoritme – påregnelig?

Forvaltning vs. individ = asymmetrisk relasjon.

Taushetsbelagte opplysninger og særlige kategorier personopplysninger.

Individet påvirkes i liten grad direkte av ML-trening.

Konklusjon: formålsbegrensningsprinsippet

Vern vs. Fleksibilitet.

- Faren for formålsutglidning
- Inngrep vs. Til gunst

Behandlingsformål kan angis i lovgivningen før personopplysninger samles inn.

Taushetsplikt, jf. Fvl. §§ 13 flg.

Taushetsplikt, jf. Fvl. § 13

§ 13. ***(taushetsplikt).***

Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

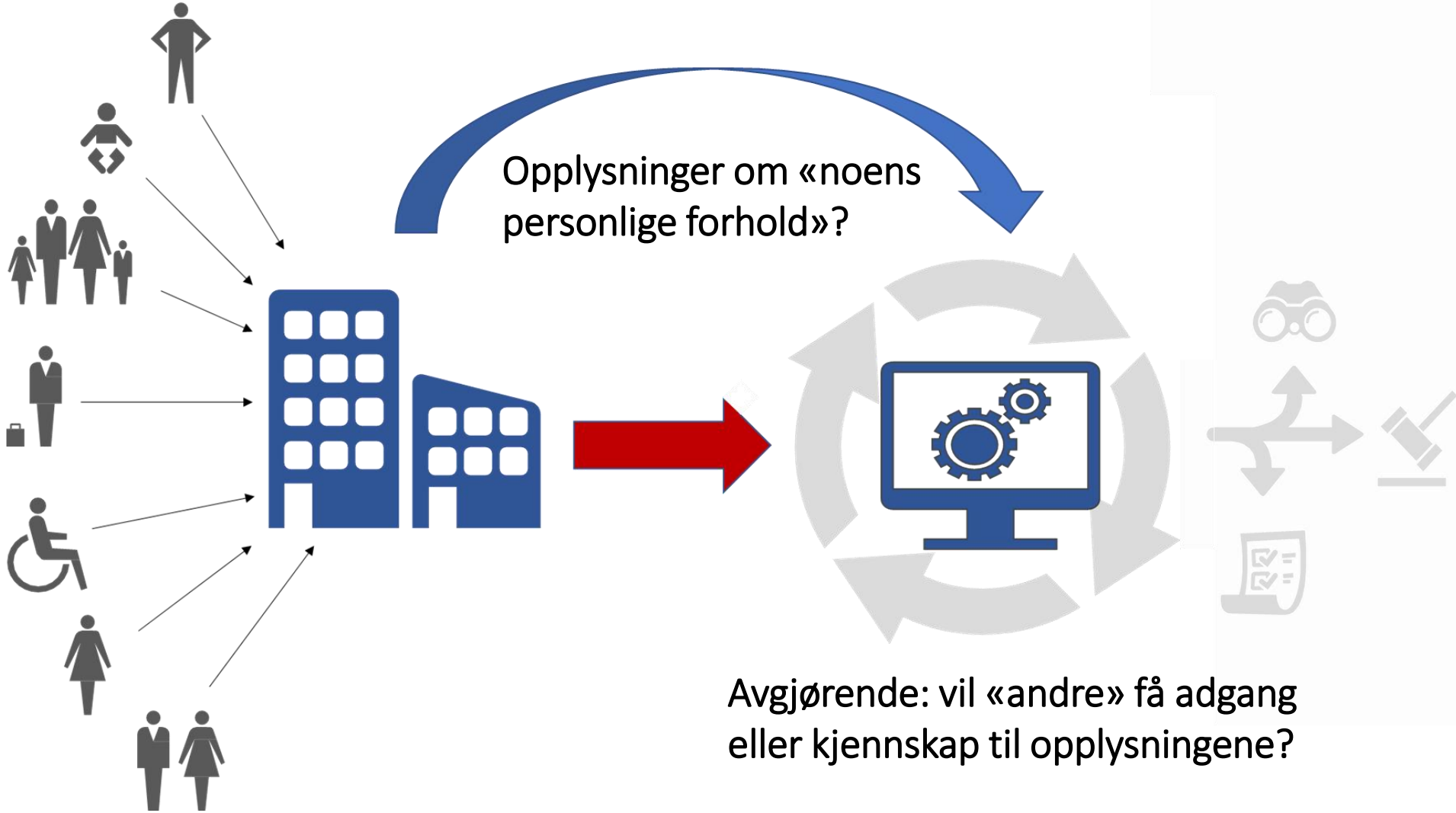
1. noens personlige forhold, eller

Hensyn: Vern av den enkelte + tillit til forvaltningen.

Innsamling av personopplysninger

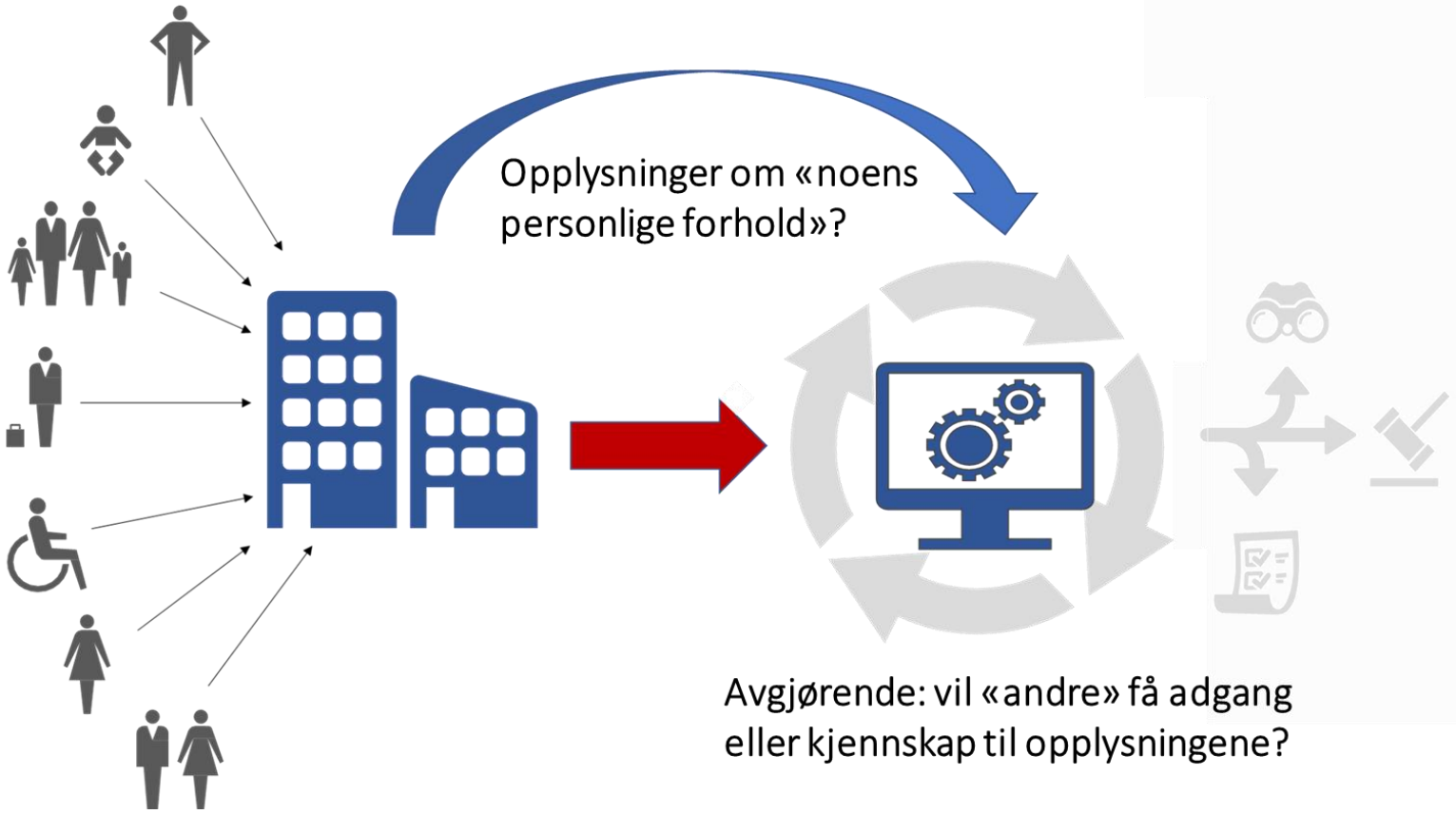
Trening av ML-algoritmer

Videre bruk i forvaltningen



Avgjørende: vil «andre» få adgang eller kjennskap til opplysningene?

Innsamling av personopplysninger Trening av ML-algoritmer Videre bruk i forvaltningen



Avgjørende: vil «andre» få adgang eller kjennskap til opplysningene?

Men: NOU 2019:5 Ny forvaltningslov

«Med «andre» menes først og fremst andre personer, men taushetsplikten må antakeligvis også gjelde overfor et datasystem.»

«Andre» omfatter også ML-systemer? Trolig ikke, jf. Hensynene bak taushetspliktreglene.

Konklusjon: taushetsplikt

Hvis taushetspliktige opplysninger – avgjørende er om «andre» vil få adgang eller kjennskap til opplysningene.

Trolig ikke grunnlag for å anvende reglene utvidende for ML-baserte datasystemer.

Relevante unntak:

- «individualiserende kjennetegn utelates», jf. Fvl. § 13 a nr. 2
  - Anonymisering eller pseudonymisering.

Kvalitet og minimering

Dataminimeringsprinsippet, jf. art. 5 (1) c

Riktighetsprinsippet, jf. art. 5 (1) d

Prinsippet om forsvarlig saksbehandling

Hvorfor er regler som stiller krav til mengde og kvalitet viktige?

Henger sammen med maskinlæringsteknologien og hvordan denne utvikles.

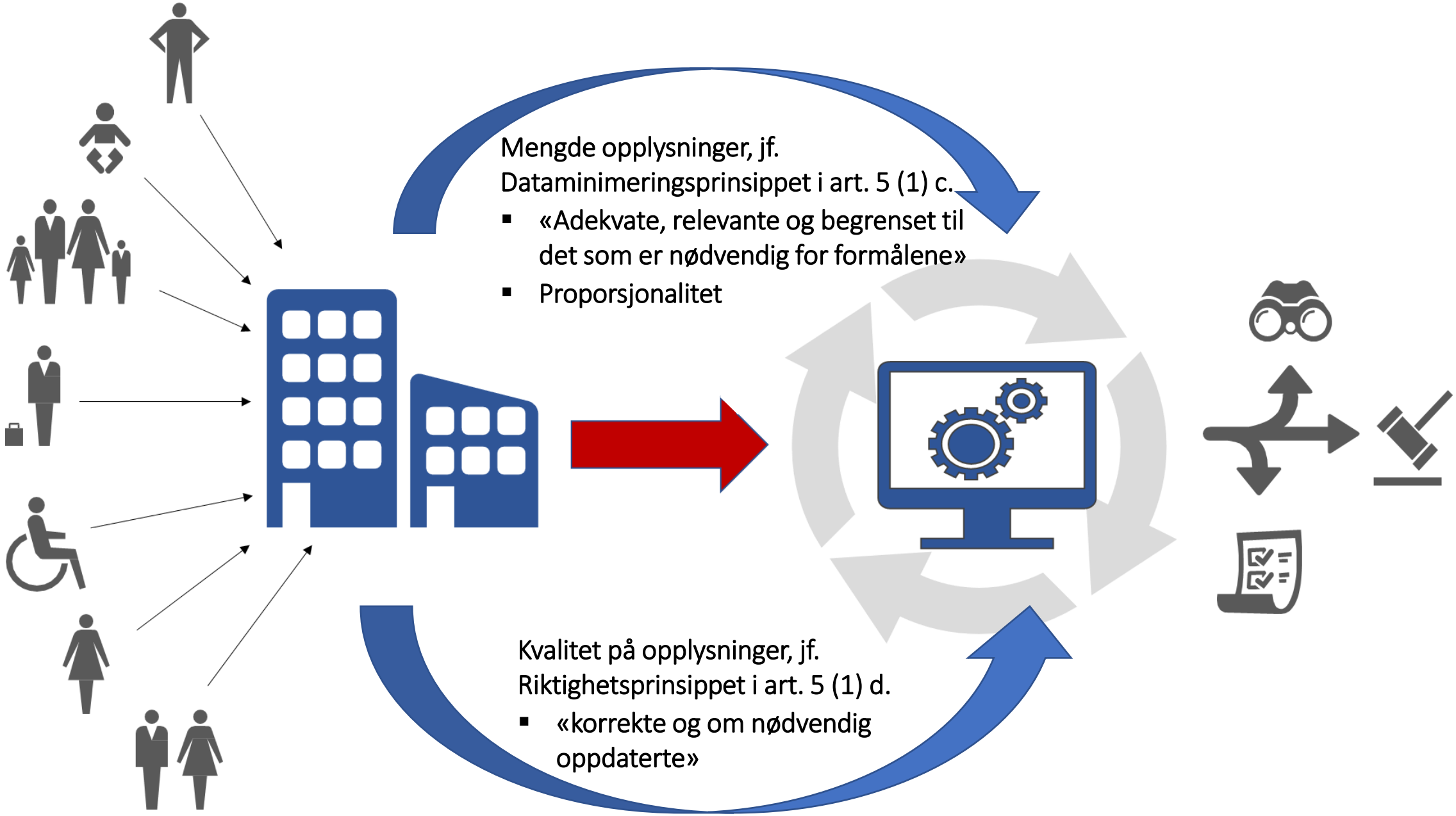
- Størrelsen på treningsmaterialet → må være tilstrekkelig for å trene en ML-algoritme.
  - Antall opplysningstyper → kjønn, alder, yrke, utdanning etc.
  - Antall av den enkelte opplysning → inntekt fra 10 år vs. 5 år.
  - Antall individer

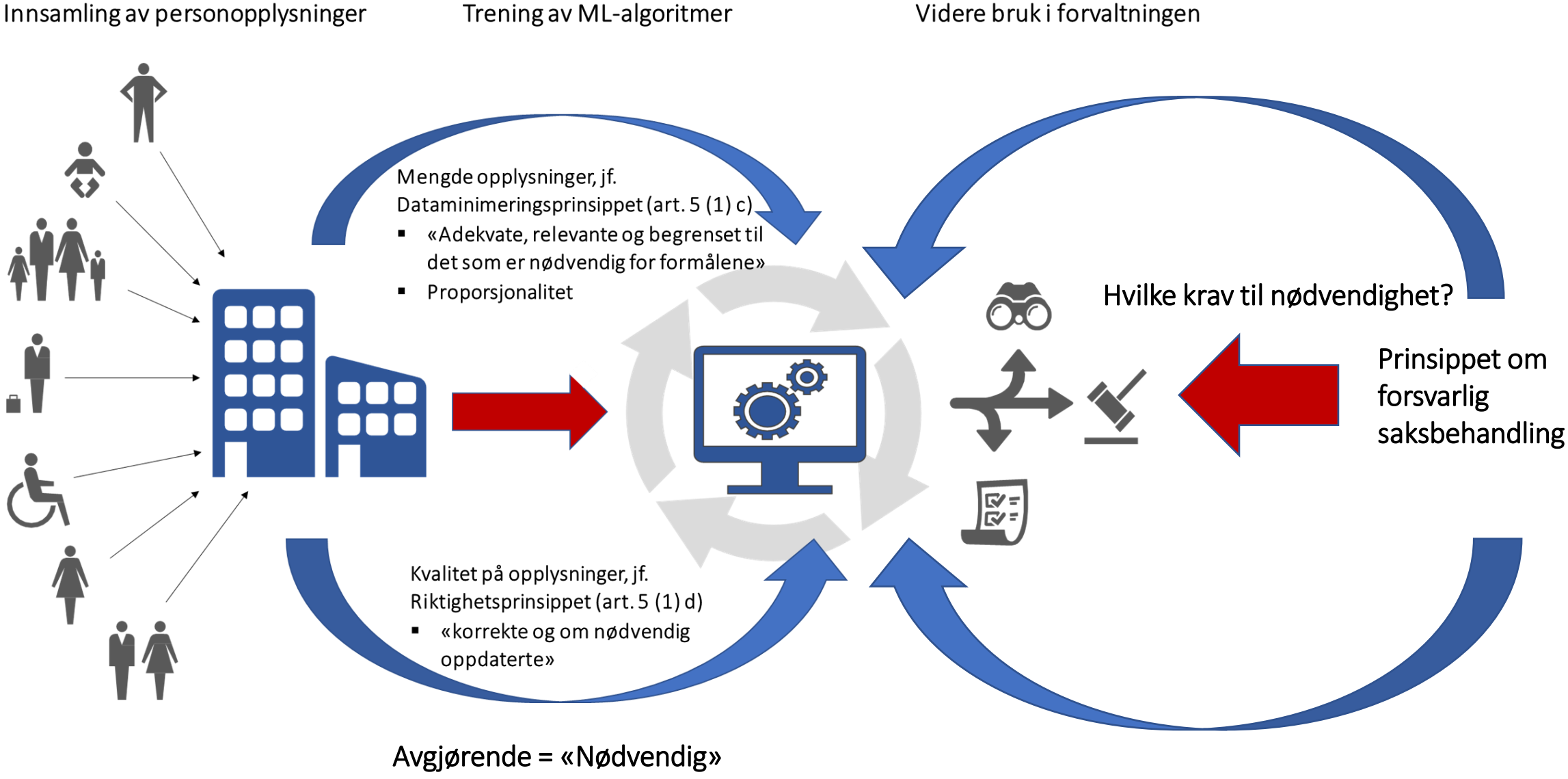
- ML-algoritmen vil speile innholdet i treningsmaterialet = «søppel inn, søppel ut».
  - Bias/skjevheter
  - Fare for feil/unøyaktigheter

Innsamling av personopplysninger

Trening av ML-algoritmer

Videre bruk i forvaltningen




Innsamling av personopplysninger
Trening av ML-algoritmer
Videre bruk i forvaltningen
Mengde opplysninger, jf. Dataminimeringsprinsippet (art. 5 (1) c)
«Adekvate, relevante og begrenset til det som er nødvendig for formålene»
Proporsjonalitet
Hvilke krav til nødvendighet?
Prinsippet om forsvarlig saksbehandling
Kvalitet på opplysninger, jf. Riktighetsprinsippet (art. 5 (1) d)
«korrekte og om nødvendig oppdaterte»
Avgjørende = «Nødvendig»

Hvilke krav må ML-baserte systemer oppfylle for at de skal være forsvarlige?

Forvaltningens virksomhet har *stor betydning* for mange mennesker.

Feil og mangler vil reproduseres og potensielt påvirke et høyt antall personer.

Digitale systemer, og ML spesielt – kan være utfordrende å oppdage feil.

Forsvarlig bruk ML i forvaltningen → strenge krav til kvalitet og pålitelighet.

Krav til mengde og kvalitet i lys av forsvarlighetskravet

Dataminimering:

- Begrensning av mengde < nøyaktighet/treffsikkerhet/representativitet
  - Men: Proporsjonalitetsprinsippet = øvre grense
- Allikevel:
  - Etterstrebe minste nødvendige mengde → gradvis utvikling
  - Anonymisering, pseudonymisering, syntetiske testdata

Riktighet:

- Riktighet av enkeltopplysninger < representativitet/kvalitet i datamaterialet generelt
  - Jf. Adekvanskravet i dataminimeringsprinsippet

Oppsummering

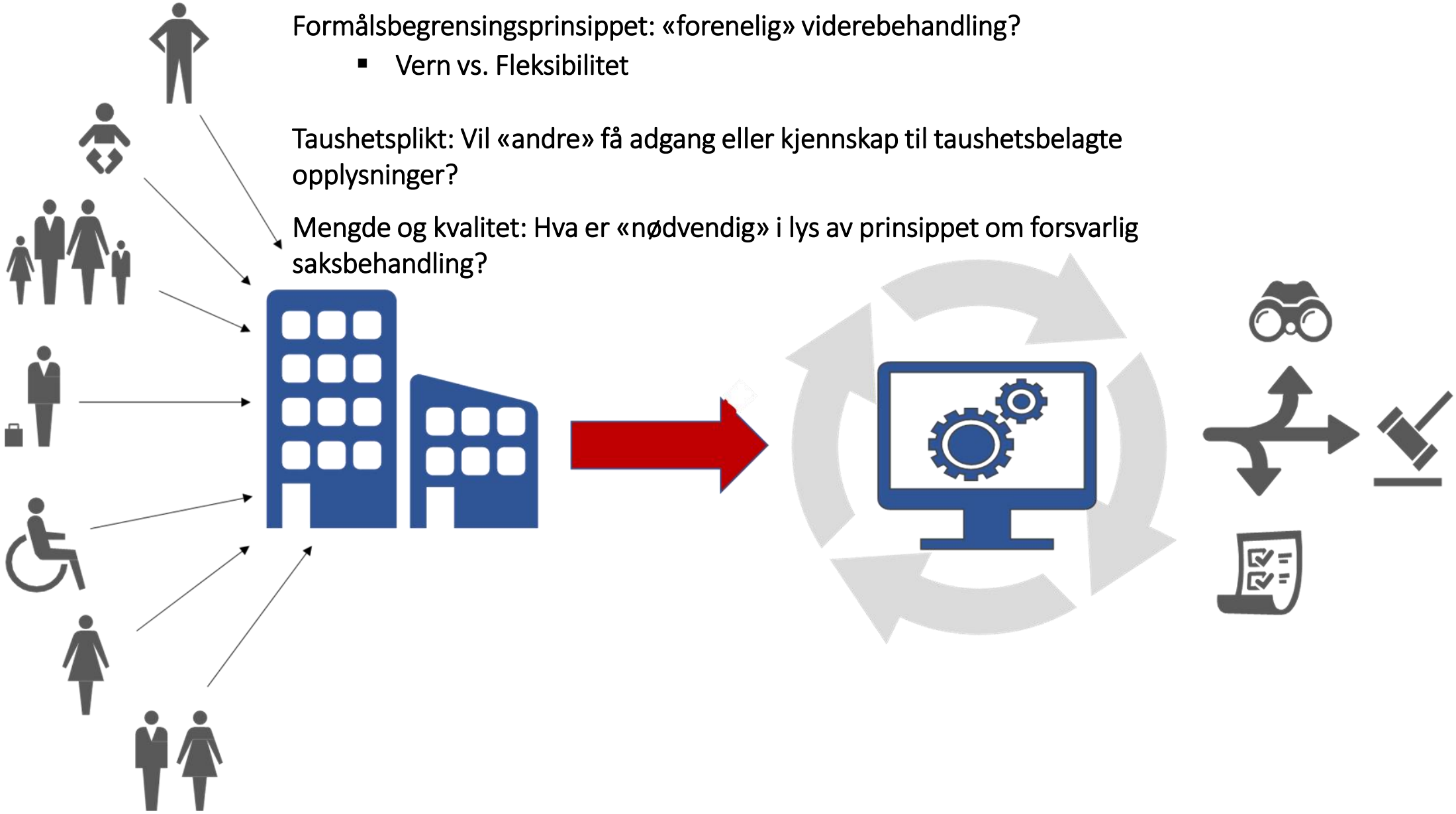
Innsamling av personopplysninger | Trening av ML-algoritmer | Videre bruk i forvaltningen

Formålsbegrensingsprinsippet: «forenelig» viderebehandling?

- Vern vs. Fleksibilitet

Taushetsplikt: Vil «andre» få adgang eller kjennskap til taushetsbelagte opplysninger?

Mengde og kvalitet: Hva er «nødvendig» i lys av prinsippet om forsvarlig saksbehandling?



Takk for meg!

JULIE LOSSIUS HUSUM

JULIE.HUSUM@GMAIL.COM