Juridiska frågor vid utveckling och användning av AI

Linda Lindström

eSam

Våra medlemmar

KUSTBEVAKNINGEN

Kriminalvården

SVA STATENS VETERINÄRMEDICINSKA ANSTALT

Statens institutions styrelse SiS

Folkhälsomyndigheten

Universitets- och högskolerådet

RÄTTSMEDICINALVERKET

ARBETSMILJÖ VERKET

SPV Statens tjänstepensionsverk

Utbetalningsmyndigheten

esv EKONOMISTYRNINGSVERKET

Havs och Vatten myndigheten

FINANSINSPEKTIONEN

csn Centrala studiestödsnämnden

Kronofogden

DOMSTOLSVERKET SVERIGES DOMSTOLAR

SWEDISH NATIONAL HERITAGE BOARD RIKSANTIKVARIEÄMBETET

Försäkringskassan

NATURVÅRDSVERKET

PENSIONSMYNDIGHETEN

Skatteverket

Riksarkivet

Sida

LANTMÄTERIET

Jordbruksverket

Skolverket

Livsmedelsverket

Länsstyrelserna

Inspektionen för vård och omsorg

eHälsomyndigheten

SCB

Tullverket

TRANSPORT STYRELSEN

tillväxtverket

TRAFIKVERKET

ARBETSFÖRMEDLINGEN SWEDISH PUBLIC EMPLOYMENT SERVICE

Boverket

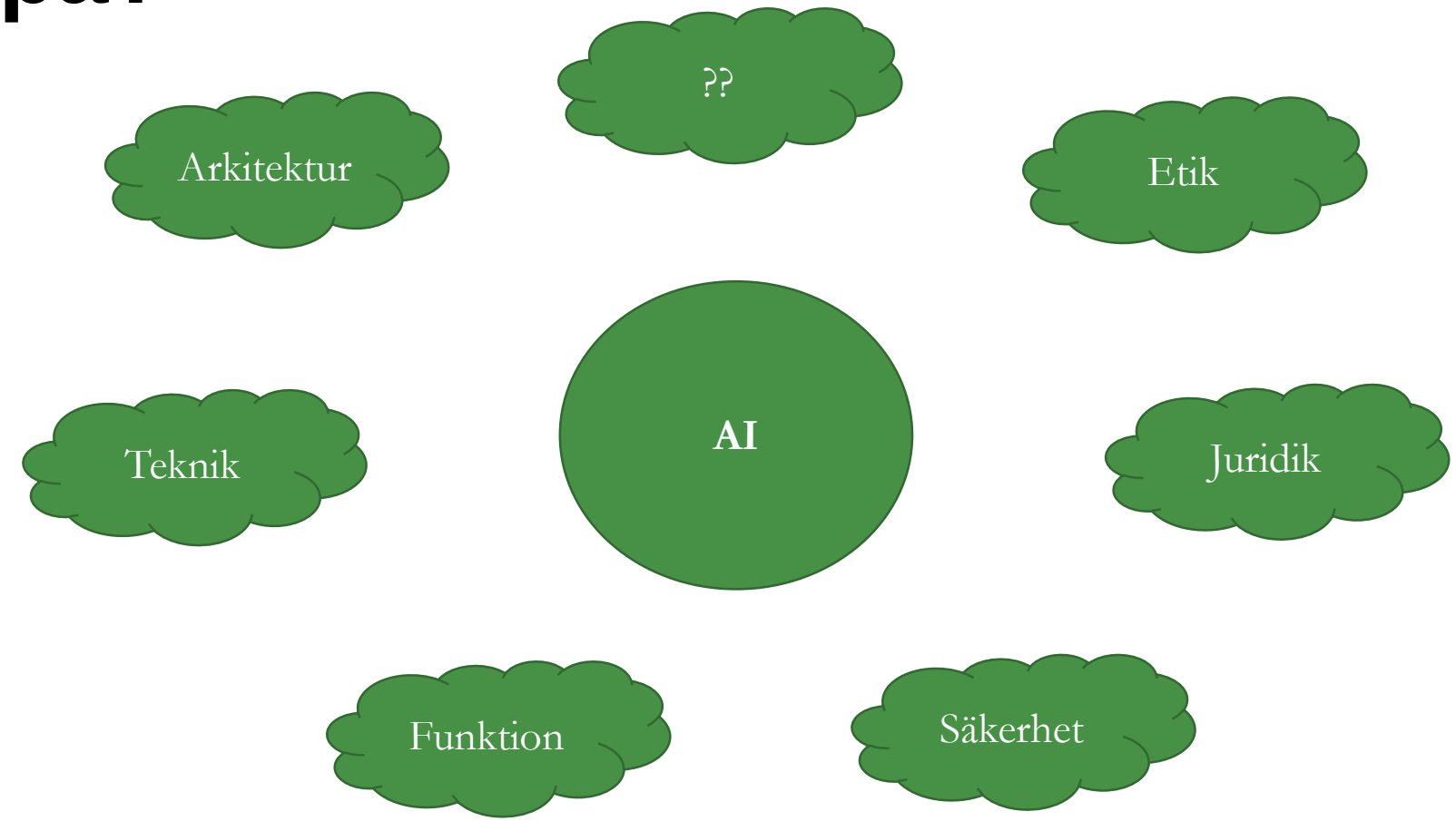
Migrationsverket

Bolagsverket

Statens servicecenter

KEMI Kemikalieinspektionen

AI-användning – vad behöver myndigheten tänka på?



Rättsliga frågor som kan aktualiseras

Rättsområden som kan aktualiseras

- AI-förordningen
  - AI-system
  - Risknivå
  - Dokumentationskrav
- Kompetensområde
  - Legalitetsprincipen – en myndighet får endast vidta åtgärder som har stöd i rättsordningen
  - Proportionalitetsprincipen
- God offentlighetsstruktur
  - Allmänna handlingar, diarieföring, gallring och arkiv
  - Upphovsrätt och vidareutnyttjande av data

Rättsområden som kan aktualiseras

- Personuppgifter
  - Rättslig grund
  - Registrerades rättigheter
  - Krav på dokumentation
  - Tekniska och organisatoriska åtgärder
  - Konsekvensbedömningar
  - Dataskyddsförordningens principer för behandling av personuppgifter måste beaktas.
- Service tillgänglighet, ärendehantering
  - Kommunicering, partsinsyn, dokumentation
  - Språk
- Informationssäkerhet
  - Informationsklassning, hot- och riskanalys
- Upphandling och konkurrensfrågor
  - It-villkor – ägandeskap, exit
- Drift och förvaltning
  - Ansvarsfrågor

Några särskilt intressanta rättsfrågor

- Transparens och förklarbarhet
- Automatiserade beslut
- Diskriminering
- Ansvar
- Testverksamhet

Transparens och förklarbarhet

- Vid AI-användning behöver det säkerställas att myndigheten klart och tydligt kan redogöra på vilka grunder ett beslut har fattats enligt förvaltningslagen.
- Behöver säkerställas att myndigheten behandlar personuppgifter på ett lagligt, korrekt och öppet sätt och ger tydlig information om den behandling av personuppgifter som sker enligt dataskyddsförordningen.
- Artikel-29-gruppens riktlinjer automatiserat beslutsfattande och profilering. Behövs nödvändigtvis inte en komplex förklaring av de algoritmer som används eller att lämna ut den fullständiga algoritmen. Men den information som tillhandahålls bör vara tillräckligt heltäckande för att den registrerade ska förstå skälen till beslutet.
- Ju mer avancerad AI, desto mer komplex blir frågan om transparens och förklarbarhet.

Automatiserade beslut

- Med automatiserat beslutsfattande avses beslut som fattas maskinellt utan att någon enskild befattningshavare på myndigheten tar aktiv del i själva beslutsfattandet i det enskilda fallet.
- Automatiserade beslut kan fattas med eller utan profilering. Vidare kan profilering ske utan att det fattas ett automatiserat beslut.
- I dataskyddsförordningen finns regler som begränsar möjligheten att använda AI för automatiserat beslutsfattande.
- Undantag i förvaltningslagen.

Diskriminering

- Risk för diskriminering vid AI-användning kan uppstå t.ex. på grund av
  - bristande kvalitet i data,
  - bristande träning av AI
  - bristande transparens och svarta lådor.
- Vid en AI-användning behöver de olika formerna för diskriminering beaktas och användningen av AI bedömas utifrån samtliga diskrimineringsgrunder i diskrimineringslagen (2008:567).

Ansvar

- Ansvar:
  - Hantering av risk för kränkningar av grundläggande fri- och rättigheter (inklusive skydd av personuppgifter, integritet och icke-diskriminering)
  - men även reglering av konsumentskydd, produktsäkerhet och produktansvar (inklusive reglering av person eller sakskador).
- I dataskyddsförordningen har den personuppgiftsansvarige ett ansvar för och ska kunna visa att principerna för behandling av personuppgifter efterlevs. Överträdelser av dataskyddsförordningen kan medföra sanktioner, inklusive administrativa sanktionsavgifter och/eller att skadestånd behöver betalas till personer som lidit skada.
- AI-förordningen har liknande sanktionsmöjligheter som i dataskyddsförordningen.
- Det är viktigt att ansvarsförhållandena säkerställs och att det är tydligt vem som bär ansvaret vid en AI-användning.

Testverksamhet

- Behov:
  - Utveckla algoritmer, träna modeller, optimera parametrar, validera kvalitet på data och modeller m.m. inom en utforskande aktivitet, inför ett beslut om eventuellt genomförande i verksamheten
  - Testa en AI-produkt innan införskaffande
  - M.m.

- Ur juridiskt perspektiv saknas ofta betydelse om det är fråga om en behandling i testmiljö eller produktionsmiljö och samma rättsområden aktualiseras.
- Informationsmängden avgörande.
- Frågor om rättslig grund, transparens, konsekvensbedömning m.m. aktualiseras.
- AI-regulatoriska sandlådor.

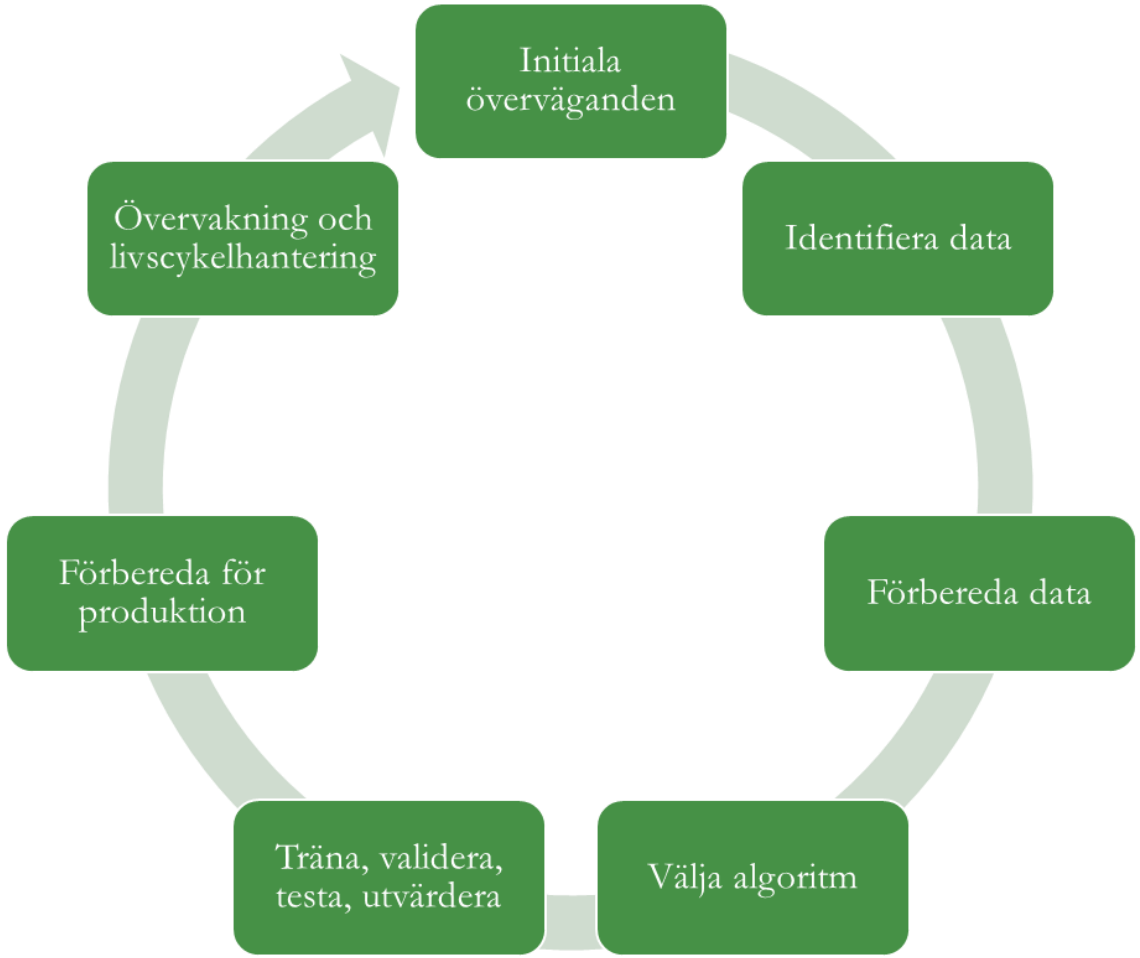
Hur kommer de juridiska frågorna in vid användning och utveckling av AI?

Två framgångsfaktorer

- Tillämpa en utvecklingsprocess/anskaffningsprocess
- God kontroll och styrning på sin data

Generell utvecklingsprocess

- Initiala överväganden inför en AI/ML-utveckling
- Beskrivning av de olika utvecklingsstegen
  - Identifiera och samla in data
  - Förbereda data
  - Välja algoritm, modell
  - Träna, validera och testa samt utvärdera och finjustera
  - Förbereda för produktion och förvaltning samt driftsätta
- Övervakning och livscykelhantering av AI-system i produktion och förvaltning



Utvecklingsprocess

Initiala överväganden inför en AI-utveckling

- Inom uppdraget?
- Kan vi?
- Bör vi?
- Legalitet
- Införskaffa?
- Etik

Övervakning och livscykelhantering av AI-system i förvaltning och produktion

- Drift
- Utvärdering
- Uppföljning
- Övervakning

Utvecklingsstegen

Identifiera data

Datakällor

Användning, rättslig grund, kvalitet m.m.

Förbereda data

Utforska | Variabler | Rensa

Rättslig grund, kvalitet m.m.

Dela upp data för träning, validering och test

Välja algoritm

Vilket problem ska lösas?

Övervakad, oövervakad, förstärkning

Förklarbarhet
Icke-diskriminering

Träna, validera, testa, utvärdera

Lärande algoritm

Rättslig grund, säkerhet m.m.

Tränings-data

Validerings-data

Testdata

Träna modell → Validera modell → Testa modell → Modell klar för produktion

Utvärdera/ Finjustera

Utvärdera/ Finjustera

Utvärdera/ Finjustera

Förbereda för produktion

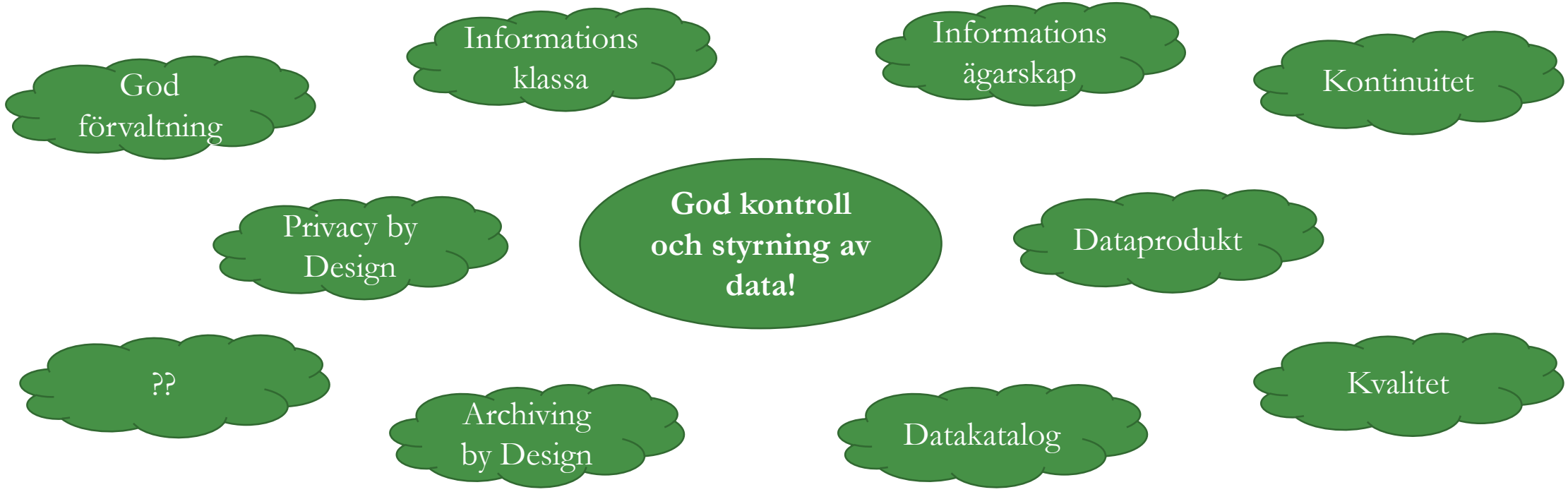
- Ansvar
- Budget
- Riskanalys
- Kommunikation

Iterera tills modellen är tillräckligt bra

Förklarbarhet, tillförlitlighet och icke-diskriminering

- Komplexa modeller med låg förklarhet resulterar ofta i noggrannare förutsägelser, varför valet av algoritmen ofta innebär en avvägning mellan hög förklarbarhet och hög träffsäkerhet
- Generell förklarbarhet respektive individuell förklarbarhet
- Tillförlitlighet innebär att egenskapsvariablerna t.ex. ger en hög andel korrekta klassificeringar och en låg andel felaktiga klassificeringar för en grupp utan jämförelse med vad som gäller för en annan grupp
- Med icke-diskriminering (fairness) menas istället att varken direkt eller indirekt diskriminering förekommer
- När man mäter förekomst att diskriminering måste det tas i beaktande att det kan finnas flera intuitivt giltiga definitioner av icke-diskriminering och att definitionerna inte kommer att peka åt samma håll

Datahantering och informationsstyrning



Summering

- Identifiera frågeställningarna – juridiska och andra
- Bemanna med rätt kompetens – laginsats!
- Gemensam begreppslära
- Tillämpa en utvecklingsprocess/anskaffningsprocess
- God kontroll och styrning av data/information

Några av eSams produkter inom AI och data

- Checklista Rättsliga förutsättningar i utvecklingsinsatser 2.0
- ES2022-01 Vägledning Pseudonymisering av personuppgifter
- ES2022-02 Vägledning Bedömning och utveckling av chattbotar
- ES2022-07 Vägledning Innovation i en myndighet
- ES2023-04 Råd praktisk användning av vägledning för innovation
- ES2022-06 Promemoria En modern registerförfattning
- ES2022-08 Checklista Juridik vid användning av AI
- ES2022-03 Rapport Samverkan kring tillämpad AI
- ES2023-2 PM Stordataanalyser och datasjöar - begrepp och rättsliga förutsättningar
- ES2023-05 Råd Intern kommunikation och användning av AI-baserade chattbotar
- ES2024-01 Rapport AI – Utvecklingsprocessen och data
- ES2024-08 Rapport Stärkt förmåga till AI i samverkan
- ES2024-09 Rapport Referensarkitektur: Datahantering och utbyte av data mellan myndigheter
- ES2024-10 Rapport Beskrivning av datakatalog
- ES2024-11 Rapport Dataprodukt och dataproduktsspecifikation
- ES2024-14 Delrapport AI-regulatorisk sandlåda – en första iteration

TACK!

Linda Lindström

esamverka.se

eSam