AI GOVERNANCE FÖR KOMMUNER

Jakob Söderbaum, dataskyddsstrateg Sundbybergs stad

2026-06-01

Agenda

1. Om AI och personuppgifters betydelse i sammanhanget
2. AI-förordningen och GDPR
3. ”AI governance” – exempel på utvärderingsprocess

1. Om AI och personuppgifters betydelse i sammanhanget

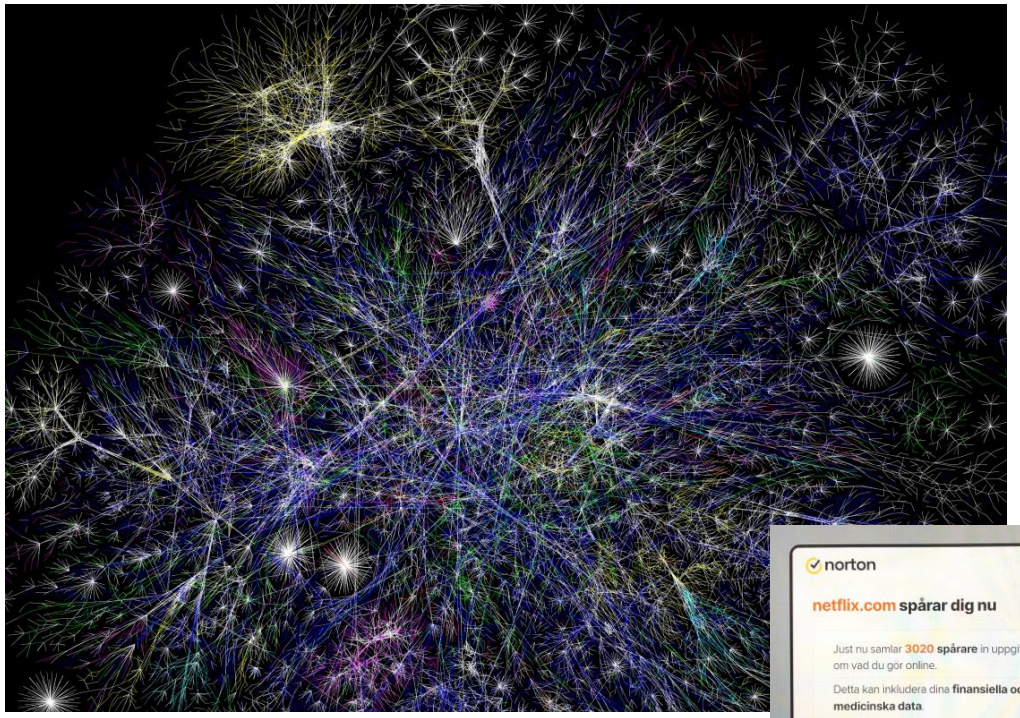
Personuppgifter är en global de facto-valuta

Det är inte bara risken för intrång och behovet av IT-säkerhet som är stort idag.

De flesta företag som säljer IT-system som inte är dyra per användare har affärsmodeller där de tankar ner mängder av Dina personuppgifter och säljer vidare till alltifrån andra företag till organiserade kriminella och stater som letar efter politiska dissidenter som flytt.

Källor:

- EU betraktar personuppgifter som en *de facto*-valuta
- Appar säljer vidare användardata
- Organiserade kriminella använder personuppgifter för att hitta lämpliga personer att begå brott mot
- Flyktingar från Kina förföljs i Sverige



Internet i dataflöden. Bild: WikiCommons Public Domain

Mönstertolkning av data

Mönstertolkning handlar inte bara om att spåra och dra nytta av personuppgifter och annan värdefull data. Genom korrekta slutsatser genererar det också nya personuppgifter:

"Facebook Likes can be used to automatically and accurately predict a range of highly sensitive personal attributes including:

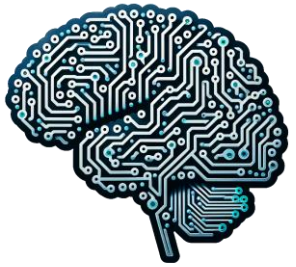
- *sexual orientation,*
- *ethnicity,*
- *religious and political views,*
- *personality traits,*
- *intelligence,*
- *happiness,*
- *use of addictive substances,*
- *parental separation,*
- *age,*
- *and gender."*

Michal Kosinski, associate professor of Organizational Behavior, Stanford University

År: 2013

Källa:
https://www.pnas.org/doi/abs/10.1073/pnas.1218772110

Om AI



Vad är AI?

- Machine Learning – *1959*
- Advanced Machine Learning
- Artificial Intelligence
- Artificial General Intelligence – *framtiden?*

Enligt **AI-förordningen** artikel 3.1 är ett ”AI-system” följande:

”ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.”

Övergripande

Fördelarna med AI är i princip också nackdelarna:

- **Mönstertolkning** är det stora nyckelordet ifråga om AI ur GDPR-synvinkel. Detta inkluderar förutsägelser och prognostisering och att skräddarsy övertygande kommunikation. Mönstertolkning är på så vis både:
    - Värdet
    - Hotet

  …och AI kan inte bara användas för att tjäna pengar på mer omfattande, bättre och snabbare mönstertolkning. Det handlar också om att **genom automatisering påverka folks beteende** i den verkliga världen (jfr Cambridge Analytica).

- **Spårbarhet** rörande personuppgifter är både det som:
    - Utgör vår möjlighet att få till stånd ett ännu bättre dataskydd med hjälp av AI; och
    - Utgör hotbilden med AI ur GDPR-synvinkel

- **Mer data leder till bättre precision** för AI-lösningar – detta är ett av skälen till jakten på data i världen.

AI-utvecklingen i USA har nu blivit gränslös

21 januari: Trump upphäver Bidens tidigare PO om begränsningar för AI-utvecklingen

Under intryck av att ett antal amerikanska tech-ledare gått ut i en debattartikel om behovet av att begränsa AI-utvecklingen, genomförde f.d. president Biden tidigare en sådan begränsning bl.a. för "national security interests" i form av en s.k. Presidential Order. Denna har nu president Trump upphävt.

Källa: https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/

→ ***Dataskyddsstrategens slutsats:*** Med dessa amerikanska säkerhetsåtgärder ute ur bilden, har vi i EU framöver behov av att vara ännu mer noggranna ifråga om utvärdering, avtalsinnehåll och användande avseende amerikanska AI-lösningar.

2. AI-förordningen och GDPR

AI-förordningen

EU:s nya AI-förordning (AI act)

- ✓ Den är uttryckligen ett komplement till GDPR.
- ✓ Den 1/8 2024 trädde AI-förordningen ikraft som svensk lag.
- ✓ Fr.o.m. 2/2 2025 gäller dess regler avseende förbjudna system.
- ✓ Fr.o.m. 2 augusti 2027 gäller dessa regler för ”leverantörer” av AI-lösningar som är på marknad 2 augusti 2025.
- ✓ De flesta övriga bestämmelser gäller från den 2 augusti 2026.
- ✓ AI-system i bruk av ”tillhandahållare” (ej ”leverantörer”) inom offentlig sektor före den 2 augusti 2026 riskerar inte sanktionsavgifter förrän den 2 augusti 2030 (artikel 113.2).

Att bedöma enligt AI-förordningen

a) Bedöm vad själva AI-lösningen har för formell risknivå.

→ Högrisk-lösningar medför behov av närmare utredning

b) Bedöm vad vår användning av AI-lösningen och den information vi lägger in i den medför att vi hamnar i för risknivå.

→ Högrisk-användande medför behov av djupare och mer komplex utredning (med många undantag och undantag till undantagen)

c) Bedöm om vi är ”tillhandahållare” eller ”leverantör” ifråga om hur vi använder den här AI-lösningen.

→ ”Leverantörer” har betydligt högre och mer omfattande krav på sig än ”tillhandahållare”

d) Bedöm säkerhetsrisker utifrån AI-förordningen, GDPR, TF och OSL (m.fl. lagar) och formulera kravställan utifrån detta! Bedöm sedan vilka säkerhetsrisker vi har kvar efter kravställan, och hur ställer vi oss till dessa.

Ansvar för behandling av personuppgifter

Vad är en personuppgift?

- Vad som helst som kan kopplas till en fysisk person

När behandlas personuppgifter?

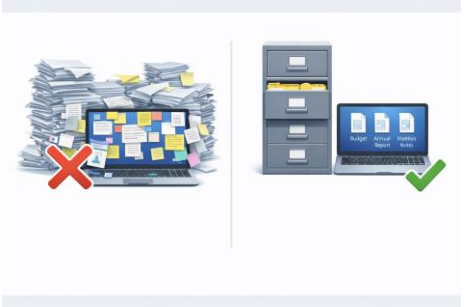
- Automatiserat eller registrerade och strukturerade personuppgifter

När får personuppgifter behandlas?

- Bara om man har både ändamål och laglig grund

Vem är ”personuppgiftsansvarig”?

- Den organisation som har bestämmande inflytande över ändamålen och medlen med behandlingen. I en kommun är det respektive nämnd.



Övergripande

Hur GDPR generellt begränsar användande av AI-lösningar inom EU:

- Genom att reglera **vad** och **hur** vi får behandla individuellt spårbar data.
- Genom att uppställa **hinder mot obehörig tillgång** och därigenom försvåra massexploatering av personuppgifter (jfr ”data harvesting” och tränande av AI-modeller).
- Genom att vara **inriktad på säker lagring och transfer av personuppgifter** i det digitala informationsbaserade samhället där AI nu växer fram.
- Genom att **AI-lösningar har förmåga att generera nya personuppgifter** på ett sätt som är svårt att både förutse och ta kontroll över.
- Genom att vi är skyldiga att **genomföra en risk- och konsekvensbedömning** (DPIA) om det **finns ”en hög risk”** för de registrerades rättigheter och friheter enligt GDPR. Vi kan i samband med detta också bli skyldiga att begära förhandssamråd från tillsynsmyndigheten innan vi påbörjar behandling av personuppgifter också i en AI-lösning.

Exempel: GDPR hindrar användande av AI

ChatGPT

Open AI, företaget bakom bl.a. ChatGPT, är inte självcertifierat enligt DPF och omfattas därmed inte av adekvansbeslutet. De har stött på patrull ur GDPR-synvinkel runtom i EU, t.ex. i Frankrike, Italien, Polen, Spanien och Tyskland. De anklagas för att bryta mot GDPR i termer av bristande…

- laglig grund
- berättigande ifråga om sina angivna ändamål
- transparens
- möjligheter att tillgodose de registrerades rätt till tillgång (registerutdrag)
- Inbyggt dataskydd (de verkar snarare ha motsatsen till “privacy by design”)

Detta utgör alltså brott mot GDPR:s artiklar 5.1.a, 12, 15, 16 och 25.1.

Se t.ex.: https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher/

DPIA: Ska alltid göras för högrisk-system!

GDPR artikel 35.1:

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

AI-risker ur kommunal synvinkel

- Verktyget genererar **nya personuppgifter** – *Utan att den registrerade har kontroll över det.*
- Verktyget drar **felaktiga slutsatser** – *”Hallucinationer”, felaktiga personuppgifter genereras.*
- Verktyget **diskriminerar** – *Rationaliteten leder till förbiseende eller kränkningar.*
- **Otillbörlig påverkan** på data – *Data kopplas ihop, ny data genereras – och en ny helhetsbild framträder efter visst användande av verktyget (”Deep Learning”) som medför av PUA oönskad påverkan på innehållet.*
- Verktyget kan fatta **felaktiga beslut** – *Den information som finns att tillgå är otillräcklig eller inte tillräckligt kvalificerad.*
- Användandet av verktyget kan medföra **konfidentialitetsbrott** – *T.ex. sekretess eller affärshemligheter tillgängliggörs för obehöriga.*

DPIA: Helhetsbild

- ✓ Lämpliga kompetenser för PUA att ha med: GDPR-kunniga, verksamhetskunniga, systemförvaltare. I förekommande fall även leverantören.
- ✓ Bedöms riskerna vara höga så måste förhandssamråd med IMY göras enligt artikel 36 GDPR.
- ✓ Sanktionsavgifter för att inte ha genomfört DPIA är 10 mkr enligt Dataskyddslagen 6 kap 2 § 2 st.

DPIA steg 1-7: Extra AI-frågor att bedöma

Syfte och förutsättningar

- Vilka mål ska användningen av AI uppnå, t.ex. vilka problem ska AI lösa? Eller vilket värde ska AI-systemet ge?
- Hur är det tänkt att AI-systemet ska användas? I vilken verksamhet och av vilka?
- Vilka personer kommer påverkas av AI-lösningen (direkt och indirekt)?

Data

- Är det rättsligt klarlagt att vi kan använda de data vi vill använda när vi utvecklar, tränar eller använder tilltänkt AI-system?
- Är de data vi har relevant, korrekt och tillräcklig och hur får vi tillgång till träningsdata om de saknas?
- Vilka risker finns det för att individer kan missgynnas av AI-systemet?

Förklarbarhet

- På vilken nivå och sätt kommer vi att behöva förklara hur systemet fungerar för utomstående?
- Hur kan vi hjälpa mottagaren att förstå/tolka svaret/resultatet från AI-systemet?

Förvaltning

- Har vi en plan för hur AI-systemet ska förvaltas, övervakas och utvärderas efter implementering?

Dessa frågor är ett urval från DIGG:s Förtroendemodell (avsedd för utvecklare) av relevans också för tillhandahållare: https://www.dataportal.se/fortroendemodellen/infor-utveckling

En komplex helhetsbedömning !

Större komplexitet i offentlig sektor än i privat sektor:

Utmaningen i en myndighet är inte bara två lagar – GDPR och AI-förordningen – som ska gå ihop…

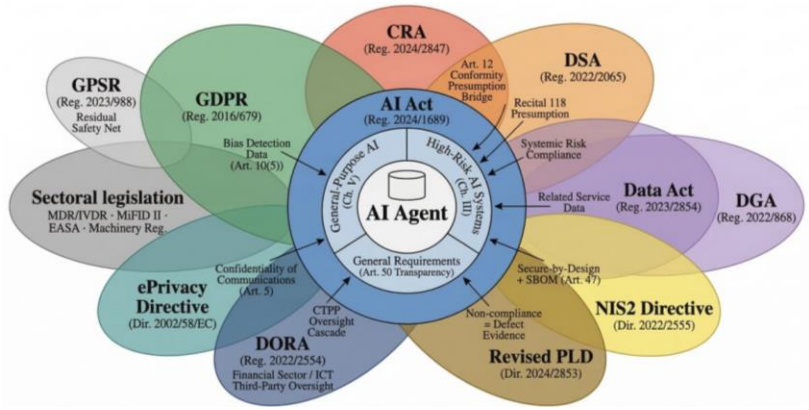
…det finns och det kommer ännu fler IT-lagar från EU som berör AI…

…den juridiska tolkningen av dessa ska både gå ihop sinsemellan och med svensk förvaltningsrätt…

…liksom med förståelse för komplexa och vitt skilda organisatoriska förutsättningar…

…och dessutom med förståelse för komplex teknik.

Det är således ganska svårt för myndigheter att ta sig igenom detta nålsöga.



3. ”AI governance” – exempel på utvärderingsprocess

Tillämpning av AI-förordningen och GDPR

5 olika juridiska bedömningar behöver göras av AI-lösningar som berör personuppgiftsbehandling:

1. Riskklassning av AI-system – *AI-förordningen*
2. Högrisk-system: Konsekvensbedömning – *AI-förordningen*
3. Lämpligt för myndigheter att undvika definieras som ”leverantör” – *AI-förordningen*
    - Höga risker
    - Omfattande krav
    - Offentlig sektor har annars ”grace period” till 2030
4. Uttolka PUA i relation till roll som ”tillhandahållare” eller ”leverantör” – *AI-förordningen och GDPR*
5. DPIA anpassad för AI-system – *GDPR och DIGG:s Förtroendemodell*

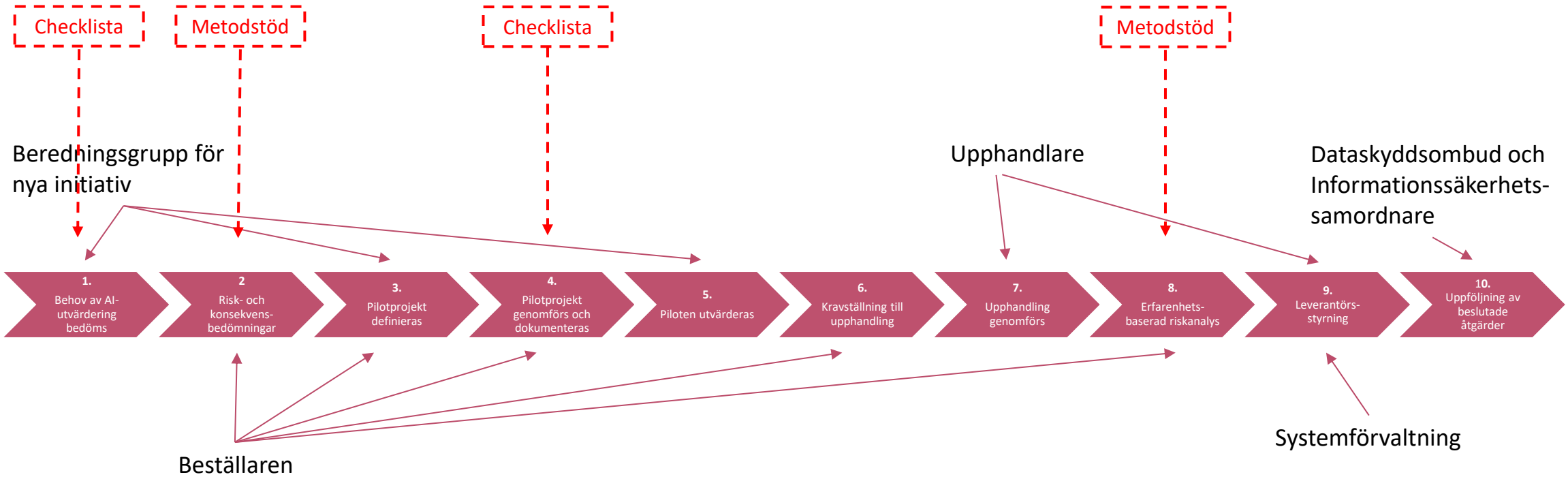
En särskild utvärderingsprocess för AI

Vad? Denna utvärderingsprocess är avsikten att **varje tilltänkt nytt AI-verktyg** i kommunen ska genomgå före det att verktyget ifråga ges full tillgång till personuppgifter, sekretessbelagd information eller högt klassade informationsmängder som kommunen har legalt ansvar för.

Hur? I processen bedöms lagenlighet (både avseende personuppgifter och sekretess!), huvudsakliga övriga **dataskydds-**, **informationssäkerhets-** och **IT-säkerhetsaspekter**, liksom påvisbar **verksamhetsnytta** och tilltänkta **driftförutsättningar.** Slutsatserna läggs till grund för ett dokumenterat riskmedvetet beslut om införande.

Varför? Eftersom vi har **komplexa** juridiska ansvarsfrågor att utreda i relation till både komplex teknik och till många olika verksamhetsförutsättningar, är det **riskabelt att låta medarbetare fritt använda AI-verktyg** som på ett eller annat sätt hanterar digital information som kommunen har ett legalt ansvar för. Kommunen (var och en av dess nämnder) ansvarar ju för brott mot TF/OSL, GDPR och AI-förordningen som utförs av medarbetare även om varken kommunens politiker eller direktörer känner till att dessa brott äger rum. Och det är **höga sanktionsavgifter** förenade med sådana brott.

Översiktsbild av processen



Särskild utvärderingsprocess i 10 steg (1/4)

Steg 1: **Beredningsgruppen bedömer om inkommet ärende utgör ett IT-system av sådant slag att det ska genomgå den särskilda processen för utvärdering av AI-lösningar (fokus på ”förbjudna system” och att ifråga om ”högrisksystem” undvika att bli ”leverantörer”).** Alla IT-system bör fr.o.m. AI-förordningens ikraftträdande betraktas som att de innehåller AI-lösningar. Sådana IT-system som bedöms höra till misstänkta högrisksystem eller förbjudna system enligt AI-förordningen, ska utvärderas enligt processen.

- *Kompetenser som medverkar i bedömningen:* Dataskyddsombud, och/eller Informationssäkerhetsansvarig och/eller Kommunjurist i samråd med övriga Beredningsgruppen.

Steg 2: **Beställaren med stöd av sakkunniga genomför DPIA enligt GDPR och AI-förordningen, konsekvensbedömning enligt AI-förordningen och heltäckande riskanalys**. Dels alla uppenbara AI-lösningar, dels alla IT-system som är nya i relation till kommunens IT-miljö ska genomgå den utökade DPIA:n. Sakkunniga stöttar och bedömer om det finns något krav på registrering enligt AI-förordningen eller på att begära förhandssamråd avseende den tilltänkta personuppgiftsbehandlingen från IMY.

- *Kompetenser som medverkar i bedömningen:* Verksamhetskunnig och systemansvarig har huvudansvar för genomförandet, med stöd av Dataskyddsombud, Informationssäkerhets-ansvarig och IT-säkerhetsansvariga i allt utom AI-konsekvensbedömningen som Kommunjuristerna stöttar med.

Särskild utvärderingsprocess i 10 steg (2/4)

Steg 3: **Beställaren och Beredningsgruppen definierar pilotprojekt** för att verifiera tilltänkt nytta och väga denna mot lagkrav och säkerhetsbehov. Specificera tilltänkt användningsområde så snävt som möjligt, informationsklassa samt fastställ ändamål och laglig grund för aktuell personuppgiftsbehandling. Kravställ på relevanta utvärderingskriterier och arbetssätt under piloten.

- *Kompetenser som medverkar i bedömningen:* Verksamhetsansvarig och systemansvarig bereder förslag för Beredningsgruppen att besluta om.

Steg 4: **Beställaren genomför pilot och dokumenterar resultatet:** Behovsdrivet användande utvärderas utifrån föridentifierade nyttor och relevanta fördefinierade risker. Vid genomförandet, undvik helst äkta personuppgifter eller åtminstone att behandla nya personuppgifter.

Steg 5: **Beredningsgruppen utvärderar piloten:** Identifiera vilka lärdomar som bör framhållas både för ärendets eventuella breddinförande och även för kommande liknande projekt. Definiera hur resultatet bör förankras med både ledning och berörda verksamheter. Uppdra åt berörd(a) beslutsfattare att bedöma eventuellt försäkringsbehov. Svårare beslut med avseende på komplexitet och/eller kända risker eskaleras till Digitaliseringsrådet.

- *Kompetenser som medverkar i bedömningen:* Beredningsgruppen.

Särskild utvärderingsprocess i 10 steg (3/4)

Steg 6: **<u>Beställaren och sakkunniga</u> kravställer upphandling: Utgå från ovanstående punkter. Arbeta gärna med standardkrav på IT-säkerhet som situationsanpassas. Fyll i PUB-avtalets Instruktionsbilaga preliminärt.**

- *Kompetenser som medverkar i bedömningen:* Verksamhetskunniga, Upphandlingsansvarig för IT, IT-driftsansvarig, Dataskyddsombud, Informationssäkerhetsansvarig och IT-säkerhetsansvarig. Helst också extern teknisk kompetens!

Steg 7: **<u>Inköpare</u> genomför upphandling** med så höga krav som möjligt i avtalen utifrån tidigare punkter (tänk både på vårt samhällsansvar som myndighet och på lärdomarnas egenvärde!), och besvara frågor från anbudsgivare.

- *Kompetenser som medverkar i bedömningen:* Upphandlingsansvarig för IT, Dataskyddsombud och Informationssäkerhetsansvarig.

Steg 8: **<u>Beställaren och sakkunniga</u> genomför erfarenhetsbaserad riskanalys** 6-12 månader efter införande av relevanta tillkommande interna tekniska och organisatoriska säkerhetsåtgärder.

- *Kompetenser som medverkar i bedömningen:* Verksamhetskunniga och systemansvariga med stöd av Dataskyddsombud, Informationssäkerhetsansvarig och IT-säkerhetsansvariga.

Särskild utvärderingsprocess i 10 steg (4/4)

Steg 9: **<u>Inköpare och objektförvaltning</u> utför leverantörsstyrning:** Följ upp att leverantören gör vad den förbundit sig till ur säkerhetssynvinkel, att vi har på plats de säkerhetsåtgärder som vi betalar för. Bedöm om det går att öka säkerhetsnivån inom ramen för befintligt avtal. Samarbeta eventuellt med leverantören om att behovsbaserat höja säkerhetsnivån utifrån vår växande erfarenhet och förståelse.

Steg 10: **<u>Dataskyddsombud och Informationssäkerhetssamordnare</u> följer upp** att de tekniska säkerhetsåtgärder som beslutats internt har implementerats, att relevanta rutiner och riktlinjer har utarbetats och fastställts formellt och att de efterlevs av dem som använder AI-lösningen.

Säkerhetsåtgärder för pilotprojekt

Dataskyddsstrategens standardrekommendationer för säkerhetsåtgärder vid genomförande av en pilot:

- Piloten genomförs i en **separat testmiljö**.
- Piloten genomförs utifrån **specifika testfall** där enbart vissa roller medverkar som också har fått informationssäkerhetsutbildning inför piloten.
- Alla medverkande har inför piloten **klassat informationen** i sina testfall (för riskbaserat urval).
- Under piloten tittar de medverkande bara på vissa **fördefinierade verksamhetsbehov, nyttor, säkerhetsförutsättningar**.
- Piloten genomförs bara under en **begränsad tid**.
- Piloten **utvärderas i efterhand** med utgångspunkt i fördefinierade tilltänkta verksamhetsbehov, nyttor, säkerhetsförutsättningar samt upptäckter inom dessa områden under pilotens genomförande.
- **Promptningshistorik (motsv.) gallras** efter projektets avslutande.
- **Ny verksamhetsspecifik bedömning inklusive riskvärdering sker inför varje ny breddning av införandet**.

Tack!

Frågor?