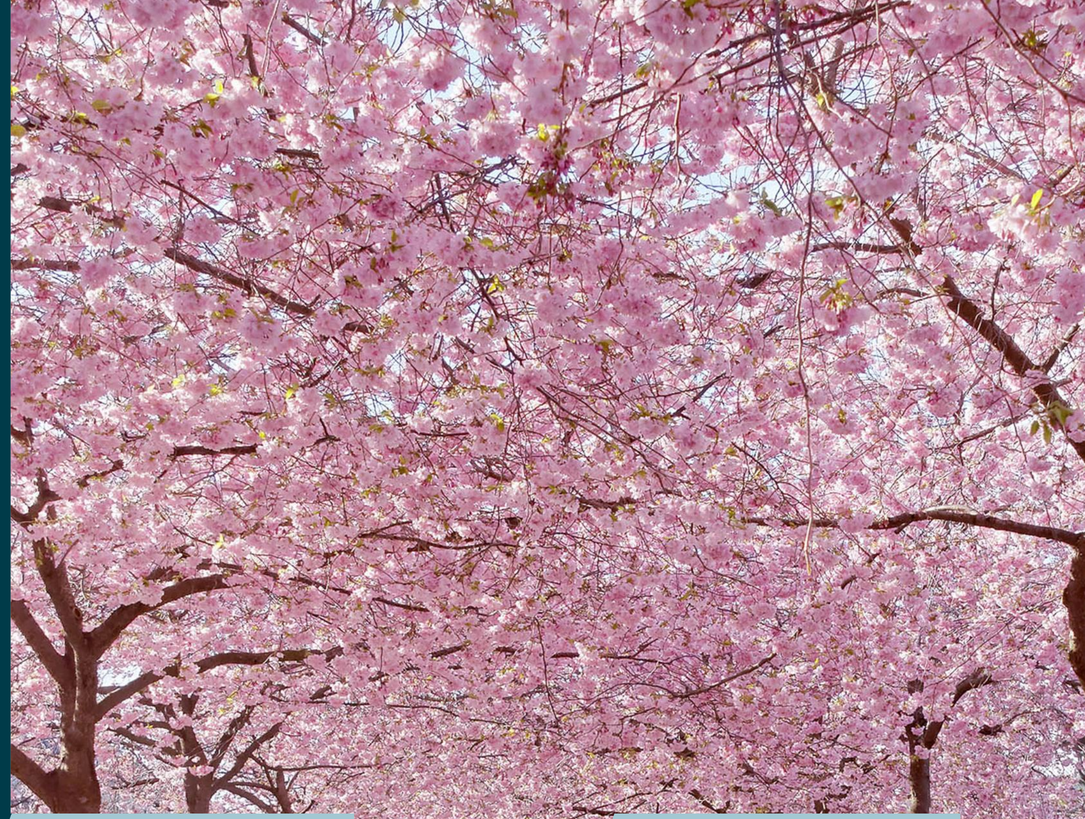
IMY. Integritetsskydds myndigheten

16 maj 2025

Nytt från IMY om den regulatoriska sandlådan och generativ AI



Inledning

Eric Leijonram
Generaldirektör

Agenda

- Senaste projekten i regulatoriska sandlådan om dataskydd
  - Projekt 3: Utlämnande av allmänna handlingar med AI
  - Projekt 4: Delning av kunduppgifter mellan banker
  - Projekt 5: Användning av personuppgifter för AI-utveckling

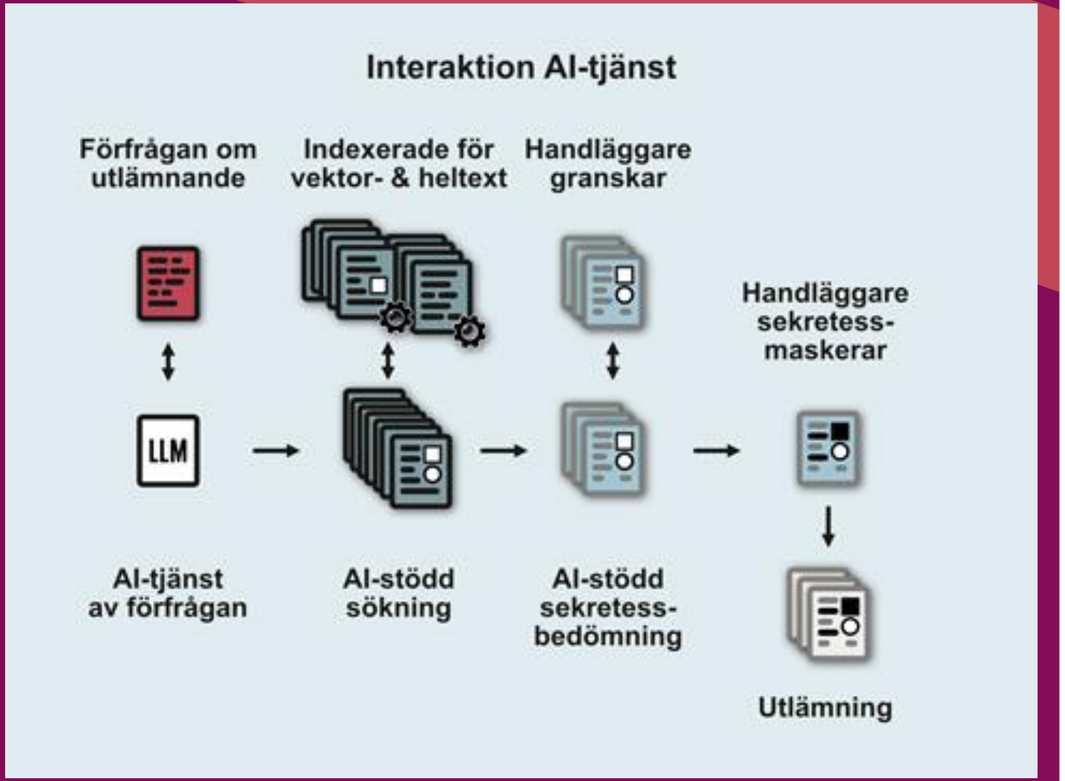
- Riktlinjer för användning av generativ AI enligt GDPR
  - Bakgrund och övergripande innehåll
  - Behöver GDPR beaktas?
  - Stöd i GDPR för användning av AI
  - Perspektiv på risker med AI
  - Allmänt tillgänglig och integrerade AI

Utlämnande av allmänna handlingar med hjälp av AI

Projekt 3 i den regulatoriska sandlådan, våren–hösten 2024

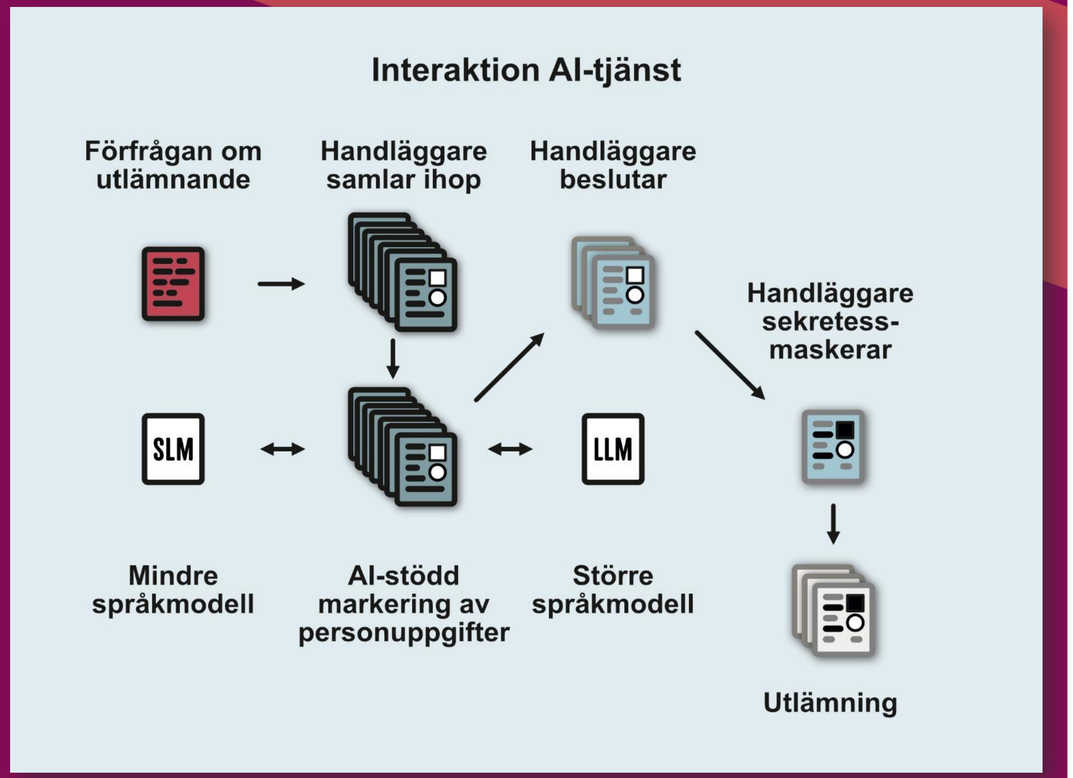
Utlämnande av allmänna handlingar med hjälp av AI

- **Deltagare:** Lidingö Stad och Atea Sverige AB med stöd av forskningsinstitutet RISE
- **Syfte:** att kunna effektivisera utlämnandeprocessen av allmänna handlingar och i högre grad kunna uppfylla det skyndsamhetskrav som tryckfrihetsförordningen (TF) ställer på offentlig verksamhet.
- **Teknik:** AI-modeller (stora och små språkmodeller) används för att analysera och sekretessmarkera personuppgifter. Handläggaren ansvarar för slutliga beslut.
- **Rapport:** Utlämnande av allmänna handlingar med hjälp av AI



Ursprungsvisionen för projektet – helhetstjänsten

- Skapa en AI-driven tjänst för att automatisera hela processen från begäran till utlämnande av handlingar. På grund av tekniska och juridiska utmaningar valde man att fokusera på maskeringstjänsten.



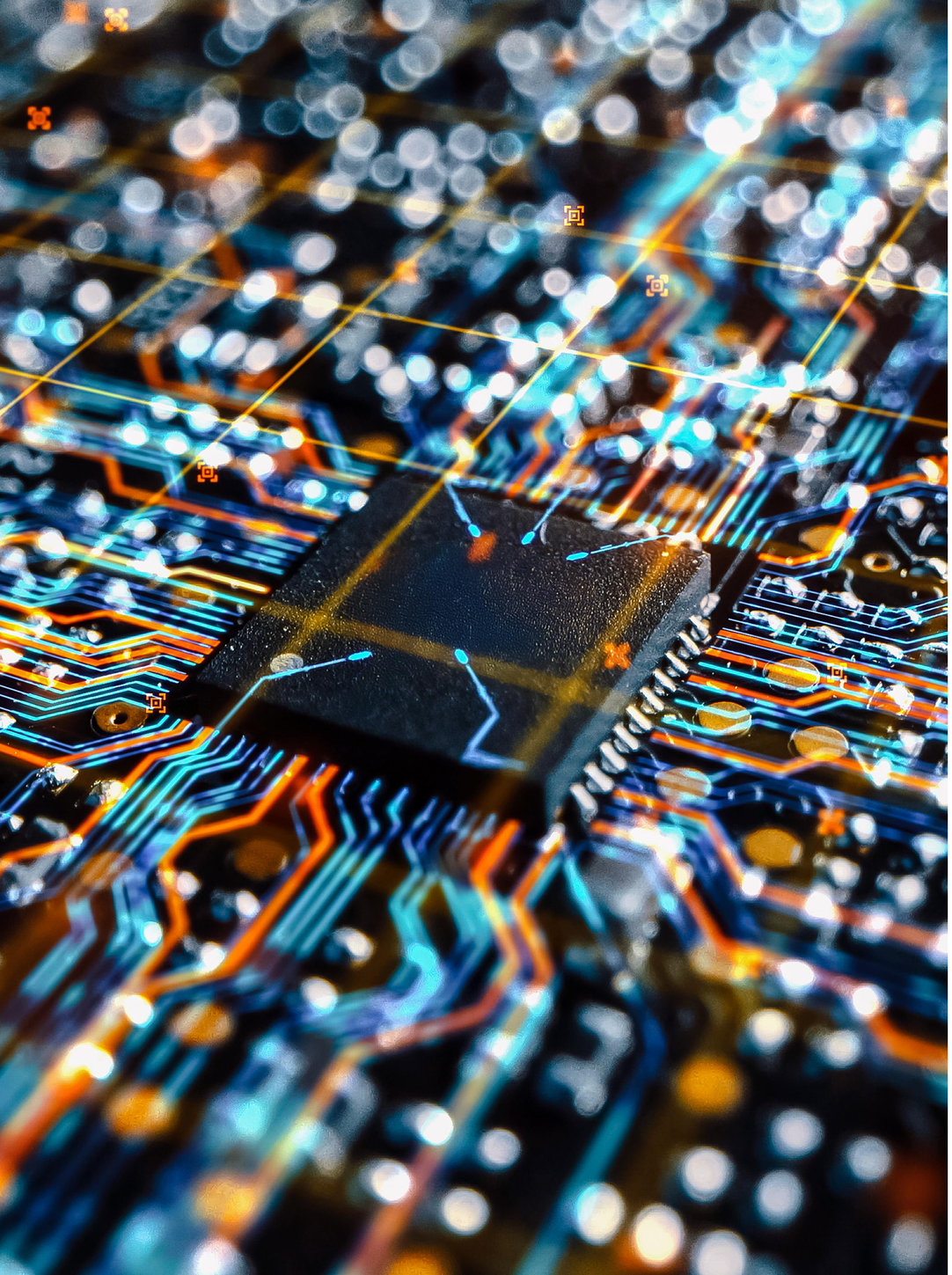
Maskeringstjänsten

- Tjänsten är utformad för att identifiera och markera både direkta och indirekta personuppgifter i handlingar. Den ger förslag på vilka uppgifter som kan omfattas av sekretess, vilket sedan granskas och beslutas av en handläggare.

- Processen sker i två steg, där en mindre språkmodell analyserar enklare personuppgifter och en större modell utför en djupare analys.

Kan AI användas för att hantera en begäran om utlämnande av allmänna handlingar?

- Vägval – hela processen eller delar av den?
- Twist på vad som är ”rutinbetonade åtgärder”
- En avancerad metod ställer högre krav



Tre medskick

- AI kan användas som ett digitalt stöd
- Börja i det mindre invecklade – och skala upp
- Behåll den mänskliga kontrollen

Ökad informationsdelning mellan banker för att stärka förmågan att bekämpa bedrägerier och penningtvätt

Projekt 4 i den regulatoriska sandlådan, hösten 2024–våren 2025

Ökad informationsdelning mellan banker för att stärka förmågan att bekämpa bedrägerier och penningtvätt

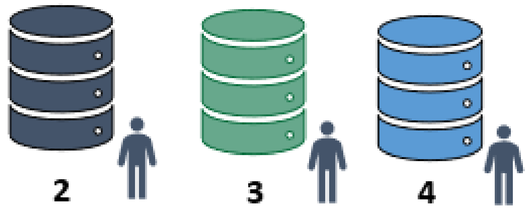
- **Deltagare**: SEB, Nordea, Swedbank och Handelsbanken
- **Syfte**: Projektet syftar till att effektivt motverka ekonomisk brottslighet, som årligen kostar Sverige 100–150 miljarder kronor, med fokus på gråzonsfrågor om dataskydd och integritet.
- **Planerad behandling**: Delning av viss kundinformation kopplat till förhöjd risk för penningtvätt, terroristfinansiering och bedrägerier i ett gemensamt system.
- **Tidsplan:** Rapport publiceras inom kort, se länk i slutet av presentationen

Tilltänkt delning av kunduppgifter i projektet

Bank 1 har en pågående kundkännedomsbedömning om Person A.

Bank 1 kan använda eventuell information från bank 2, 3 och/eller 4 om Person A i sin egen kundkännedomsbedömning och vidta adekvata åtgärder inom ramen för kundkännedomsprocessen.

Bank 1 kan ”pinga” kunden i systemet mot de övriga bankerna för att få fram information om huruvida Person A har flaggats av bank 2, 3 och/eller 4.



Bankerna 2, 3 och 4:s ”interna” data.

Alternativ 1: Delning av namn, personnummer och träff eller inte träff avseende förhöjd risk.

Alternativ 2: Delning av namn, personnummer och träff eller inte träff, plus information varför personen har flaggats.

Vilka frågor tittar vi på?

- Utgör flaggningen delning av brottsuppgifter?
- Finns det lagstöd för delningen enligt dataskyddsförordningen?

Tre medskick

- Bedömningen av vad som är brottsuppgifter är viktig
- Banksekretessen gäller parallellt med GDPR
- Lagändring krävs för tilltänkt delning

Vidarebehandling av personuppgifter för utveckling och användning av AI

Projekt 5 i den regulatoriska sandlådan, våren–hösten 2025

Vidarebehandling av personuppgifter för utveckling och användning av AI

- **Deltagare:** Familjens jurist med stöd av SynData och forskningsinstitutet RISE
- **Syfte:** Vidarebehandling av personuppgifter i syfte att effektivisera processer och förbättra klientstöd i vårdnadstvister
- **Teknik**: AI och syntetisering
- **Samhällsnytta:** Skydda barn och minska föräldrars lidande genom att undvika konflikter, forskningsunderlag
- **Tidplan:** Slutrapport preliminärt oktober 2025

Träna AI-modell med syntetiserad data

Vilka frågor tittar vi på?

- Träning av AI-modell med personuppgifter
- Syntetisera data
- Fokus på ändamålsbegränsning, rättslig grund, känsliga personuppgifter och brottsuppgifter
- Ej fokus på om anonymisering är uppnådd

Riktlinjer för användning av generativ AI enligt GDPR

Bakgrund

- Riktlinjerna togs fram inom ett så kallat regeringsuppdrag i samarbete med Myndigheten för digital förvaltning (Digg)
- Uppdraget var att *främja* användningen av generativ AI
- IMY har tagit fram de delar som rör dataskydd i riktlinjerna, se rapporten GDPR vid användning av generativ AI
- Riktlinjerna riktar sig till den offentliga förvaltningen enligt uppdraget, men kan även användas av privata aktörer
- Riktlinjerna berör användning av generativ AI – inte egen utveckling av AI eller annan AI

Övergripande innehåll

- Behöver dataskydds-regelverket beaktas?
- Enskildas rättigheter
- Rättslig stöd
- Automatiserat beslutsfattande
- Dataskyddsrättsliga principer
- Överföringar till tredjeland
- Personuppgiftsansvar
- Säkerhet
- Särskilt om användning av allmänt tillgänglig och integrerad generativ AI

Beakta GDPR som utgångspunkt

- Dataskyddsregelverket blir tillämpligt om personuppgifter behandlas vid användning av generativa AI-system
- Exempelvis gäller det när personuppgifter matas in i en prompt till en AI-modell, eller när personuppgifter efterfrågas i modellens utdata
- Personuppgifter kan också finnas inlärda i modellens grunddata, vilket innebär att dataskyddsregelverket normalt behöver beaktas

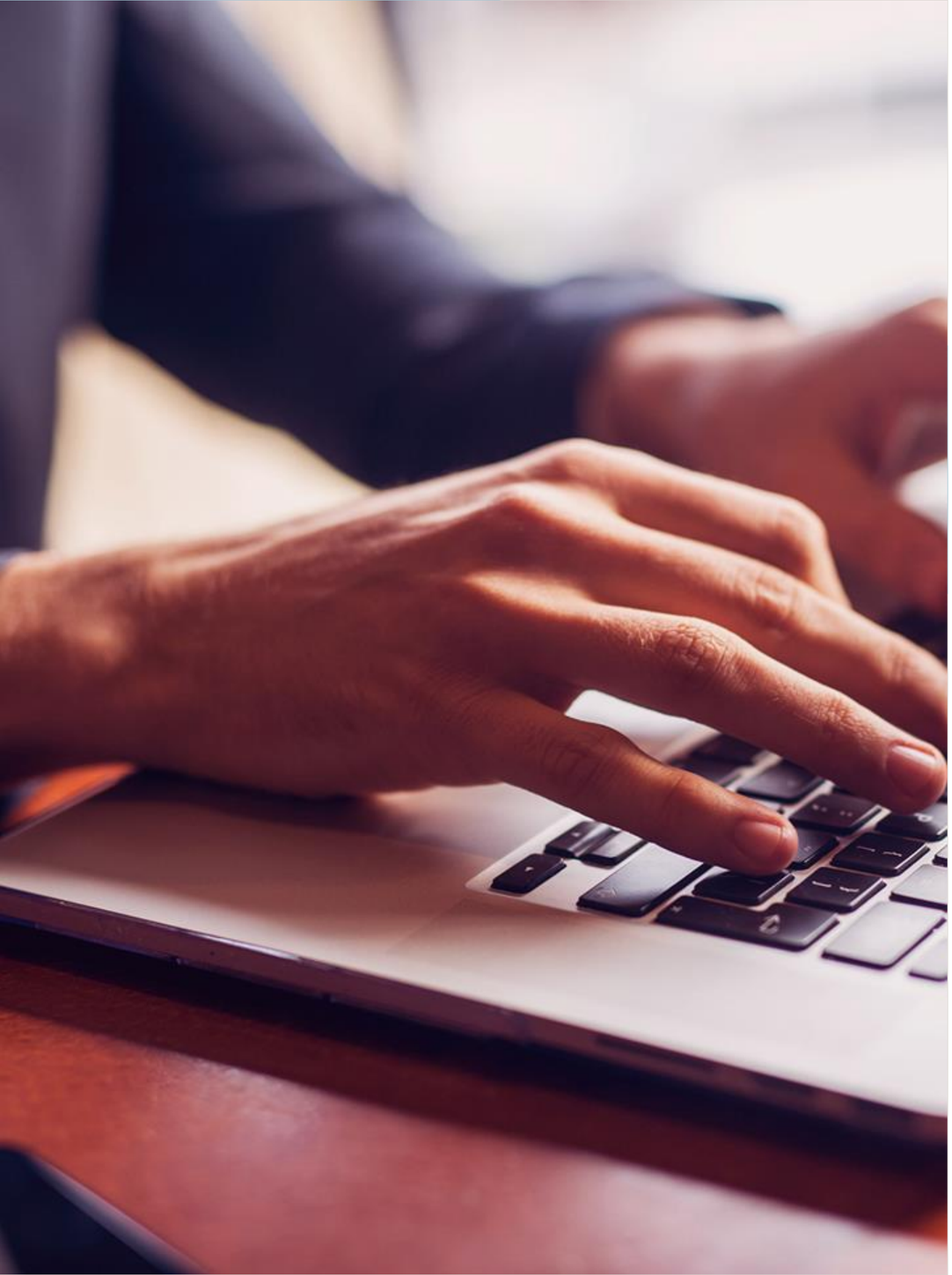
Stöd i GDPR för användning av AI

- Om generativ AI bidrar till att fullgöra en offentlig **verksamhets uppdrag** enligt lag, finns det som utgångspunkt stöd för att behandla personuppgifter med sådan teknik

- Användningen av AI behöver vara nödvändig, exempelvis för att den **effektiviserar** verksamheten

- **Ju större riskerna** med behandlingen är, **desto högre krav** på precision och tydlighet gällande den rättsliga grunden

På IMY:s webbplats finns mer vägledning om rättsligt stöd för AI även i privat verksamhet

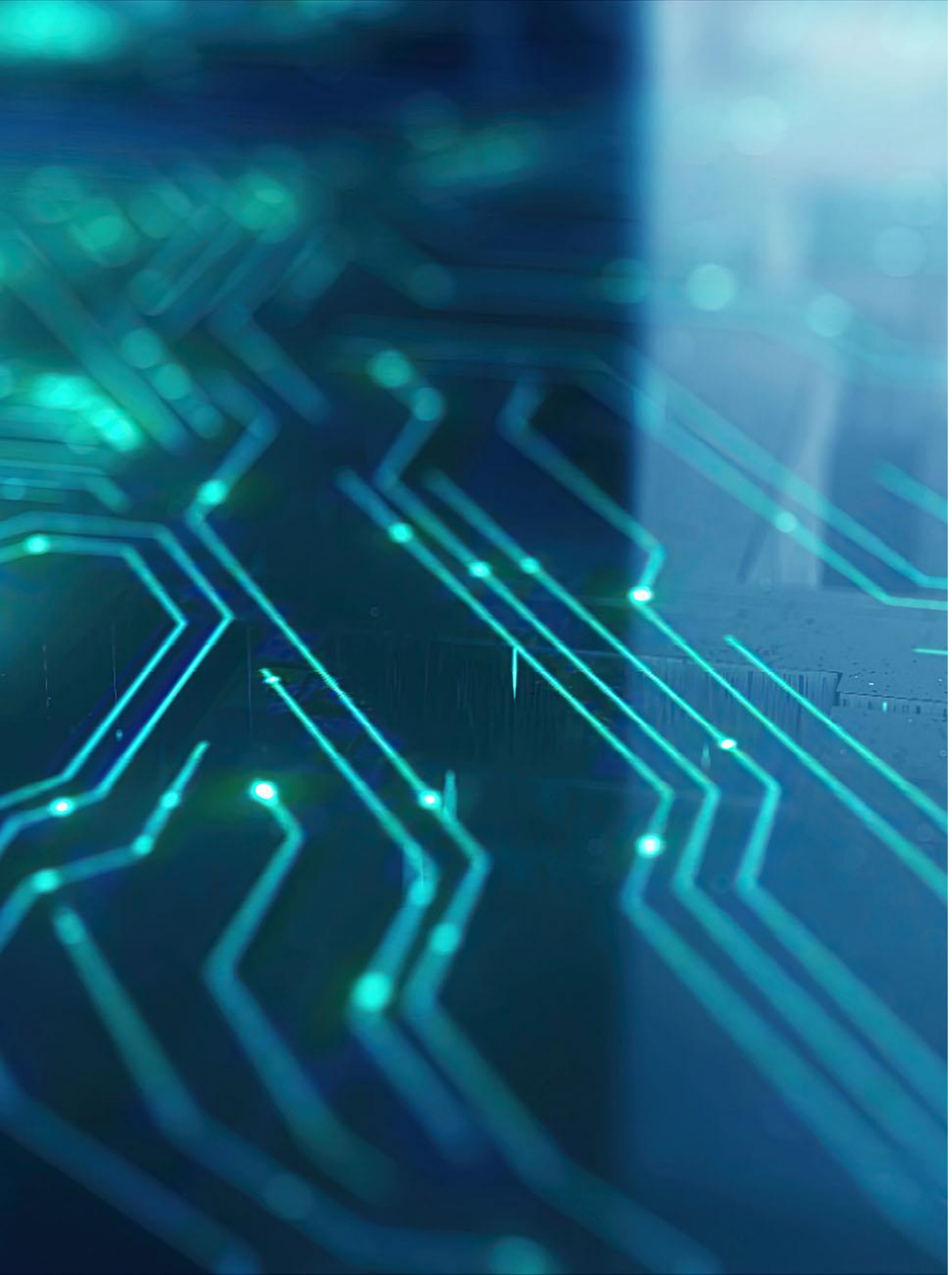


Perspektiv på risker med AI

- Tekniken normalt inte i sig en risk, utan hur den används av människor och verksamheter
- Metoden för riskhantering enligt GDPR är densamma för AI som för andra ”medel”
- Skynda långsamt – och behåll kontrollen

Allmänt tillgängliga och integrerade generativa AI-tjänster

- Ta ställning till om och hur dessa tjänster får användas i verksamheten (genom t.ex. en AI-policy)
- Bestäm vilken information tjänsten ska få tillgång till
- Innan användningen påbörjas, se till att organisationens informationshantering är god
- Många leverantörer lägger ansvaret på att användaren av tjänsten har ställt in den och använder den på ett integritetsvänligt sätt

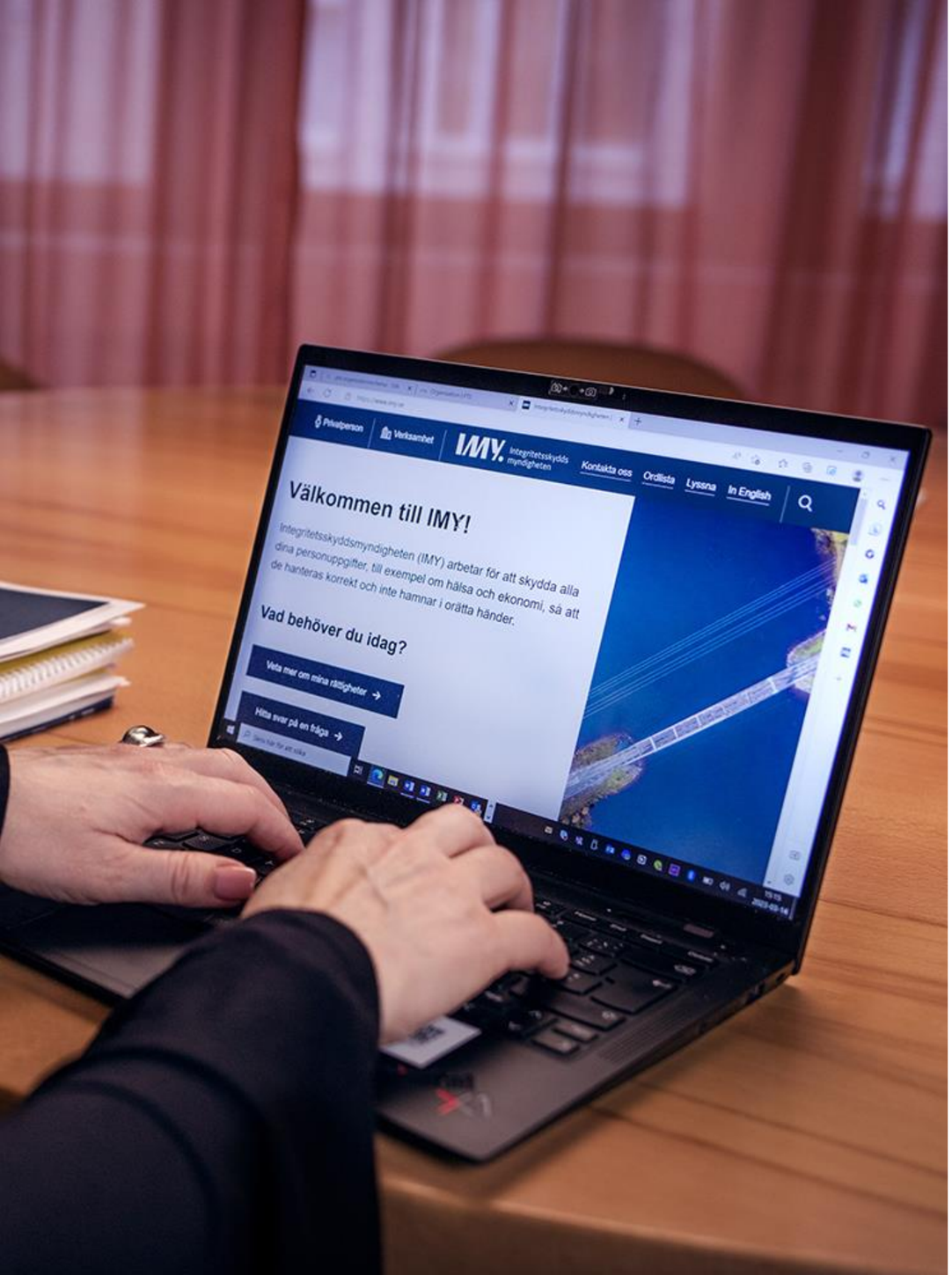


Tre medskick

- GDPR och användningen av generativ AI går att förena
- Ta ansvar för användningen och ta fram styrdokument som reglerar användningen i verksamheten
- Bedöm risker och hantera dessa kontinuerligt

Frågor?

Tack för att du lyssnat!
Svara gärna på vår utvärdering



Länkar till mer information

- Rapporter från IMY:s regulatoriska sandlåda om dataskydd
- Rapport: GDPR vid användning av generativ AI
- Vägledning om GDPR och AI på IMY.se

Presentationen skickar vi till dig tillsammans med utvärderingsenkäten.