

2024-08-28

GDPR och AI-förordningen

GDPR:s grundläggande begrepp

Facktilhörighet

Röntgenbild

Ljudinspelning

Förnamn

Politiska åsikter

Registreringsnummer

Bild

Efternamn

IP-nummer

Etniskt ursprung

Adress

Telefonnummer

Ärendenummer

Blodgrupp

Videoinspelning

DNA

Fingeravtryck

Personnummer

E-postadress

Sexuell läggning

Religiös övertygelse

Bolagsnummer

Facktilhörighet ⚠

Röntgenbild ⚠

Ljudinspelning

Förnamn

Politiska åsikter ⚠

Registreringsnummer

Bild

Efternamn

IP-nummer

Etniskt ursprung ⚠

Adress

Telefonnummer

Ärendenummer

Blodgrupp ⚠

Videoinspelning

DNA ⚠

Fingeravtryck ⚠

Personnummer

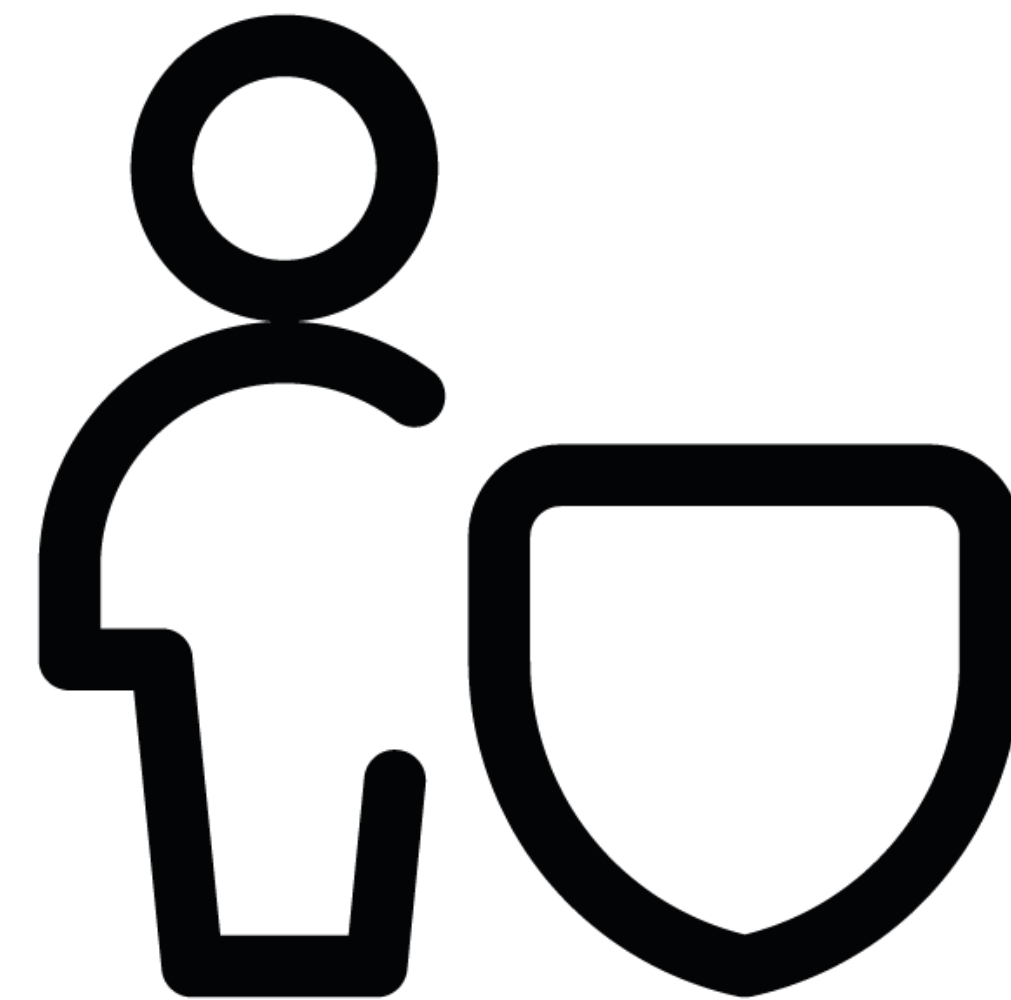
E-postadress

Sexuell läggning ⚠

Religiös övertygelse ⚠

Bolagsnummer

Registrerad



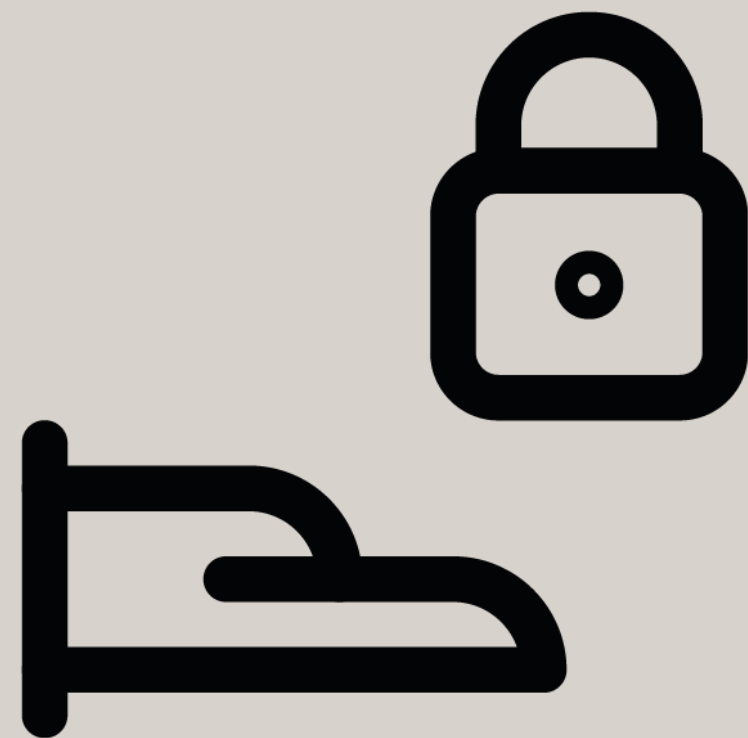
En registrerad är en person vars personuppgifter behandlas

Behandling är en åtgärd som innebär att personuppgifter...

- Samlas in
- Registreras
- Organiseras
- Struktureras
- Lagras
- Bearbetas
- Ändras
- Tas fram
- Läses
- Används
- Lämnas ut
- Överförs
- Sprids
- Justeras
- Sammanförs
- Begränsas
- Raderas
- Förstörs

Personuppgiftsansvarig

- Bestämmer
 - Vilka personuppgifter som ska behandlas
 - Varför de ska behandlas (ändamål)
 - Hur de ska behandlas (medel)

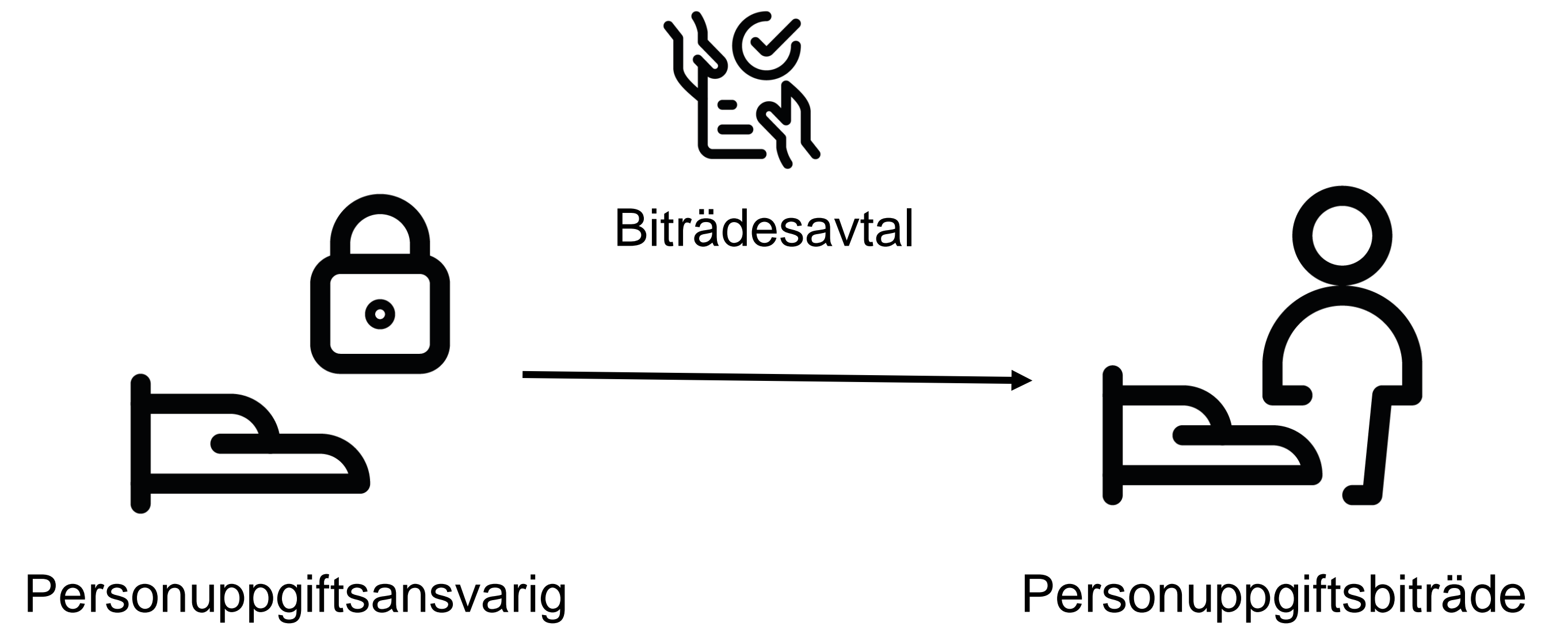




Personuppgiftsbiträde

- En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

Exempel: IT-support

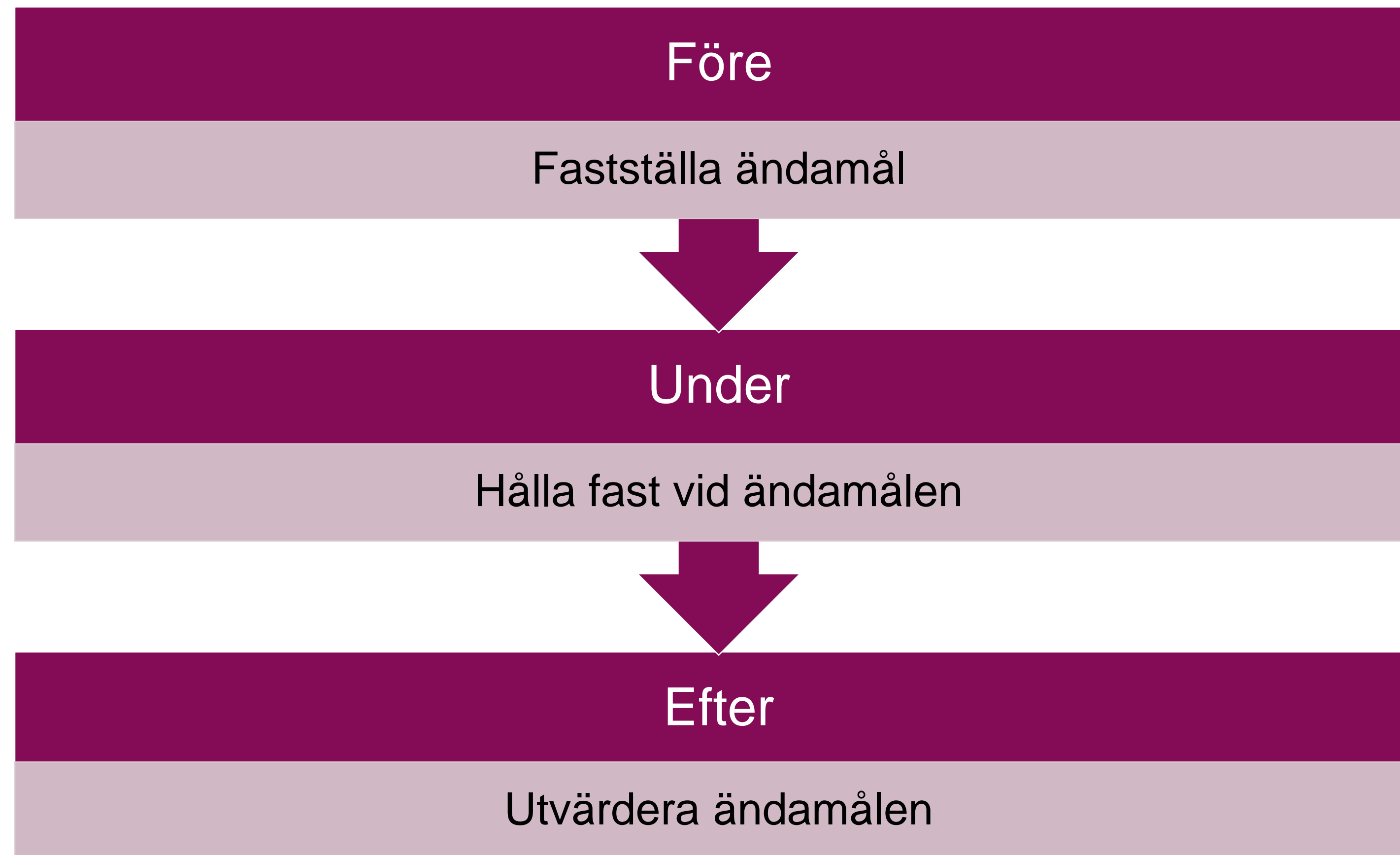


GDPR:s grundläggande principer

Laglighet, korrekthet och öppenhet

- Laglighet – Följ dataskyddslagsstiftningen!
- Korrekthet – Förutsägbarhet för den registrerade
- Öppenhet – Rätt till insyn och information

Ändamålsbegränsning





Uppgiftsminimering

- Den personuppgiftsansvariga får samla in så många personuppgifter som behövs för sina ändamål...
- ...men inte mer än så!
- Ändamålen avgör vilka och hur många uppgifter som får sparas

Riktighet

- Den personuppgiftsansvariga behöver rätta personuppgifter som är felaktiga
- Ibland kan den personuppgiftsansvariga behöva radera felaktiga personuppgifter

Lagringsminimering

- Personuppgifter får endast lagras så länge det är nödvändigt för de ändamål för vilka de samlades in



Integritet och konfidentialitet

- Ansvar att skydda personuppgifter som behandlas, både inom och utanför organisationen.



Ansvarsskyldighet

- Den personuppgiftsansvariga ska ansvara och kunna visa att man lever upp till de grundläggande principerna



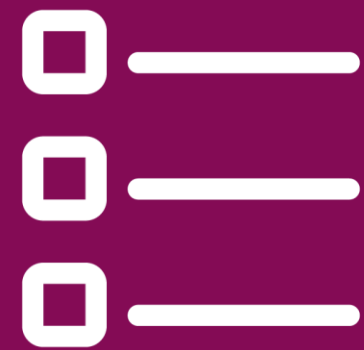
Rättslig grund enligt GDPR



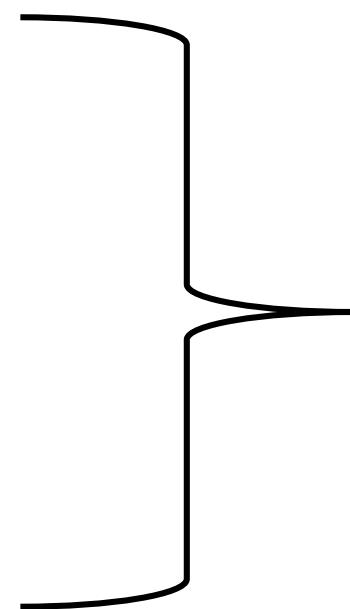
Rättsliga grunder

- Avtal
- Rättslig förpliktelse
- Samtycke
- Intresseavvägning
- Myndighetsutövning & uppgift av allmänt intresse
- Grundläggande intressen

Bestäm alltid



- Ändamålet
- Rättslig grund



- För **varje** personuppgiftsbehandling!

GDPR och AI-förordningen

Allmänt

- **GDPR**
 - EU:s allmänna regleringen av behandling av personuppgifter
 - En teknikneutral lagstiftning
 - Ska gälla parallellt med AI-förordningen
- **AI-förordningen**
 - EU:s allmänna reglering av AI
 - Reglerar AI-system och AI-modeller för allmänna ändamål
 - Hänvisar i vissa fall till GDPR:s definitioner

Exempel då AI-förordningen gäller, men inte GDPR

- Inga personuppgifter behandlas i samband med användandet av ett AI-system med hög risk

Exempel då GDPR gäller, men inte AI-förordningen

- System som inte omfattas av definitionen "AI-system" enligt AI-förordningen och som inbegriper personuppgiftsbehandling
- AI-system med låg risk som inbegriper personuppgiftsbehandling
- Högrisk-AI-system som inbegriper personuppgiftsbehandling och är i testnings- och utvecklingsstadiet och som ännu inte har släppts ut på marknaden eller tagits i bruk

Exempel då både GDPR och AI-förordningen gäller

- AI-system med hög risk som innefattar personuppgiftsbehandling

Aktörer

- **GDPR**
 - Personuppgiftsansvarig
 - Personuppgiftsbiträde
- **AI-förordningen**
 - Leverantör
 - Tillhandahållare (eng. *deployer*)

Leverantör och personuppgiftsansvarig

- Bolag A behandlar personuppgifter i samband med att träna en AI-modell för att ta fram ett nytt AI-baserat rekryteringsverktyg. Rekryteringsverktyget ska kunna hjälpa till att sortera jobbansökningar.
- Det är Bolag A som utvecklar det nya AI-baserade rekryteringsverktyget och som bestämmer hur systemet ska fungera och vilka personuppgifter som AI-modellen ska tränas på.
- Bolag A kommer att agera både som **leverantör** enligt AI-förordningen och som **personuppgiftsansvarig** enligt GDPR.

Tillhandahållare och personuppgiftsansvarig

- Bolag B köper in Bolag A:s rekryteringsverktyg. Bolaget B ska använda rekryteringsverktyget i den egna verksamheten.
- Genom att använda rekryteringsverktyget kommer Bolag B att behandla personuppgifter om de som söker jobb hos Bolag B.
- Bolag B är personuppgiftsansvarig för den personuppgiftsbehandling som sker i samband med användandet av rekryteringsverktyget.
- Bolag B kommer att agera som **tillhandahållare** enligt AI-förordningen och som **personuppgiftsansvarig** enligt GDPR.

Leverantör, tillhandahållare och personuppgiftsansvarig

- Bolag A tar fram det nya AI-baserade rekryteringsverktyget och använder också rekryteringsverktyget i den egna verksamheten.
- **Vad händer då?**

Riskbedömningar

- **Artikel 35 GDPR**
 - Konsekvensbedömning avseende dataskydd
 - Ansvarig aktör:
Personuppgiftsansvariga
- **Artikel 27 AI-förordningen**
 - Konsekvensbedömning avseende grundläggande rättigheter när det gäller AI-system med hög risk
 - Ansvarig aktör:
Tillhandahållare som är
 - *offentlighetsrättsliga organ*
 - *privata enheter som tillhandahåller offentliga tjänster*
 - *kreditgivare och liv- och sjukförsäkringsbolag (i vissa fall)*

EU-försäkran om överensstämmelse

- En leverantör av ett AI-system med hög risk ska upprätta en EU-försäkran om överensstämmelse
- Om AI-systemet inbegriper behandling av personuppgifter, ska försäkran bland annat innehålla en förklaring om att systemet uppfyller kraven i GDPR
- **Vad menas?**

Marknadskontrollmyndigheter enligt AI-förordningen

Marknadskontrollmyndighet på nationell nivå

- Artikel 70.1

Varje medlemsstat ska vid tillämpning av denna förordning som nationella behöriga myndigheter inrätta eller utse [...] **minst en marknadskontrollmyndighet.**



AI-system med hög risk enligt artikel 6.2 AI-förordningen

AI-system som omfattas av bilaga III (uppdelning i olika ämnesområden):

- **Punkt 1:** Biometri
- **Punkt 2:** Kritisk infrastruktur
- **Punkt 3:** Utbildning och yrkesutbildning
- **Punkt 4:** Sysselsättning, arbetsledning och tillgång till egenföretagande
- **Punkt 5:** Tillgång till och åtnjutande av grundläggande privata tjänster och väsentliga offentliga tjänster och förmåner
- **Punkt 6:** Brottsbekämpning
- **Punkt 7:** Migration, asyl och gränskontrollförvaltning
- **Punkt 8:** Rättskipning och demokratiska processer

Marknadskontrollmyndighet avseende AI-system som används av vissa myndigheter (1/2)

- **Artikel 74.8**

För AI-system med hög risk som förtecknas i **punkt 1 i bilaga III** ska medlemsstaterna, i den mån systemen används för brottsbekämpande ändamål, gränsförvaltning och rättvisa och demokrati, och för AI-system med hög risk som förtecknas i **punkterna 6, 7 och 8 i bilaga III** till denna förordning, till marknadskontrollmyndigheter för tillämpning av denna förordning utse antingen **de behöriga tillsynsmyndigheterna för dataskydd** enligt direktiv (EU) 2016/679 eller direktiv (EU) 2016/680 [...].

Marknadskontrollmyndighet avseende AI-system som används av vissa myndigheter (2/2)

AI-system som omfattas av bilaga III
(uppdelning i olika ämnesområden):

- **Punkt 1: Biometri**
(OBS! I den mån AI-systemen används för brottsbekämpande ändamål m.m.)
- **Punkt 2: Kritisk infrastruktur**
- **Punkt 3: Utbildning och yrkesutbildning**
- **Punkt 4: Sysselsättning, arbetsledning och tillgång till egenföretagande**
- **Punkt 5: Tillgång till och åtnjutande av grundläggande privata tjänster och väsentliga offentliga tjänster och förmåner**
- **Punkt 6: Brottsbekämpning**
- **Punkt 7: Migration, asyl och gränskontrollförvaltning**
- **Punkt 8: Rättskipning och demokratiska processer**

Regulatoriska sandlådor för AI

Regulatoriska sandlådor för AI (1/2)

- **Artikel 57.1**

Medlemsstaterna ska säkerställa att deras behöriga myndigheter inrättar **minst en regulatorisk sandlåda för AI** på nationell nivå, som ska vara i drift senast den 2 augusti 2026.

Regulatoriska sandlådor för AI (2/2)

- **Artikel 57.10**

I den mån de innovativa AI-systemen **inbegriper behandling av personuppgifter** [...] ska de nationella behöriga myndigheterna säkerställa att **de nationella dataskyddsmyndigheterna** [...] är involverade i driften av den regulatoriska sandlådan för AI [...].

Är IMY Sveriges nya AI-myndighet?

- IMY bedömer att myndigheten är lämplig att utses som nationell myndighet för AI-förordningen som helhet;
 - det underlättar för offentliga och privata aktörer om frågorna om AI med hög risk och dataskydd samlas under samma tak
 - vi har stor vana att ge vägledning i frågor om teknik och juridik samt flera etablerade arbetssätt för fördjupad vägledning



Mer information

- Vägledning om AI och GDPR på IMY:s innovationsportal (<https://www.imy.se/verksamhet/dataskydd/innovationsportalen>)
- **Kontakt oss på innovation@imy.se**

IMY. Integritetsskydds
myndigheten

www.imy.se