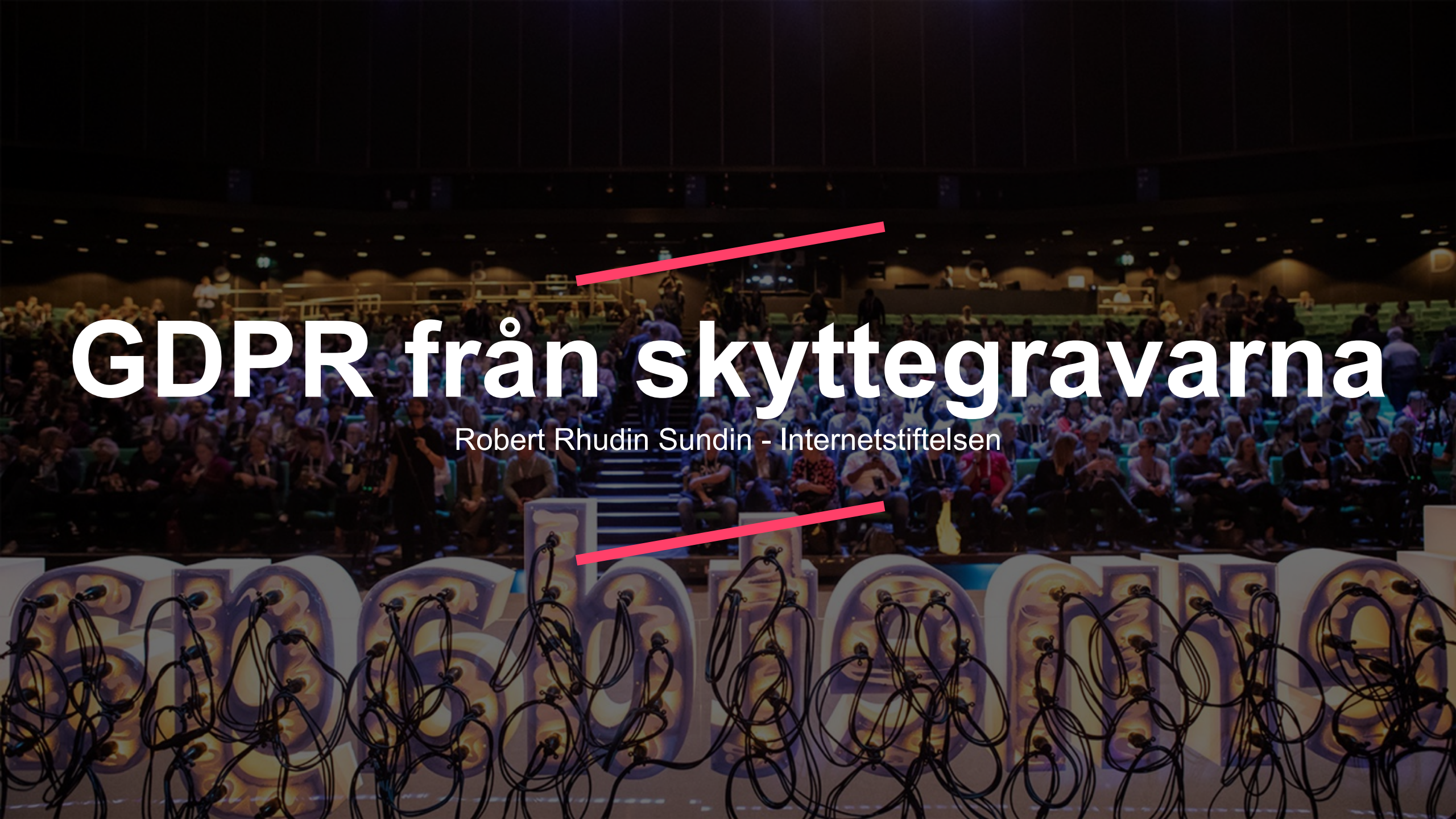




GDPR från skyttegravarna

Robert Rhudin Sundin - Internetstiftelsen

”From the trenches”

Ingen modell eller något slags facit

Så här gjorde vi utifrån våra förutsättningar
...och så här blev det

Det började så här

Hej! Fyll i det här registret med
personuppgiftsbehandlingar, syfte, laglig
grund, informationstillgångar,
gallringsrutiner, leverantörer,
konsekvensbedömningar e.t.c...



Juridik



Informationsägare



Systemägare

Okej... hur gör vi nu?

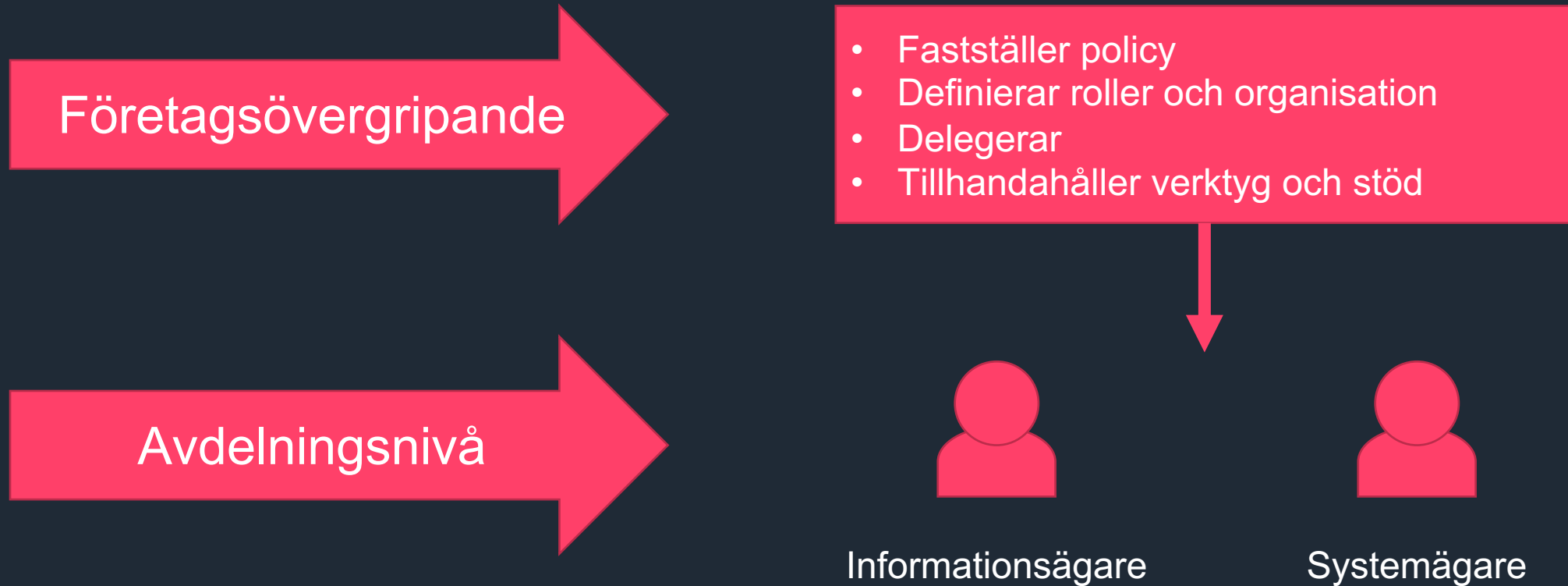
Hur identifierar vi alla PU-behandlingar och all information kring dem?

Vilka behandlingar gör vi? Vad är syftet? Vilken rättslig grund? Hur lagras uppgifter? Underleverantörer? Gallring? Med mera...

Hur håller vi arbetet levande?

Tillkommande behandlingar eller behandlingar som upphört? Ändring av behandlingar? Ändrade leverantörsförhållanden? Gallring? Med mera...

Organisation (GDPR)



Kan vi haka på befintliga rutiner?

Avdelningsnivå



Informationsägare



Process 1



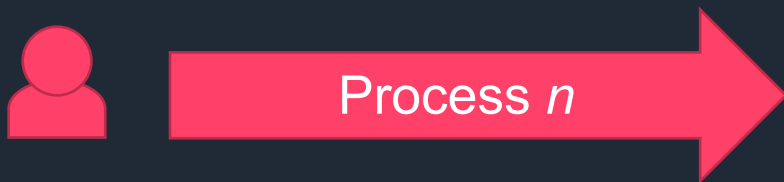
Process 2



Process 3

Informationssäkerhet

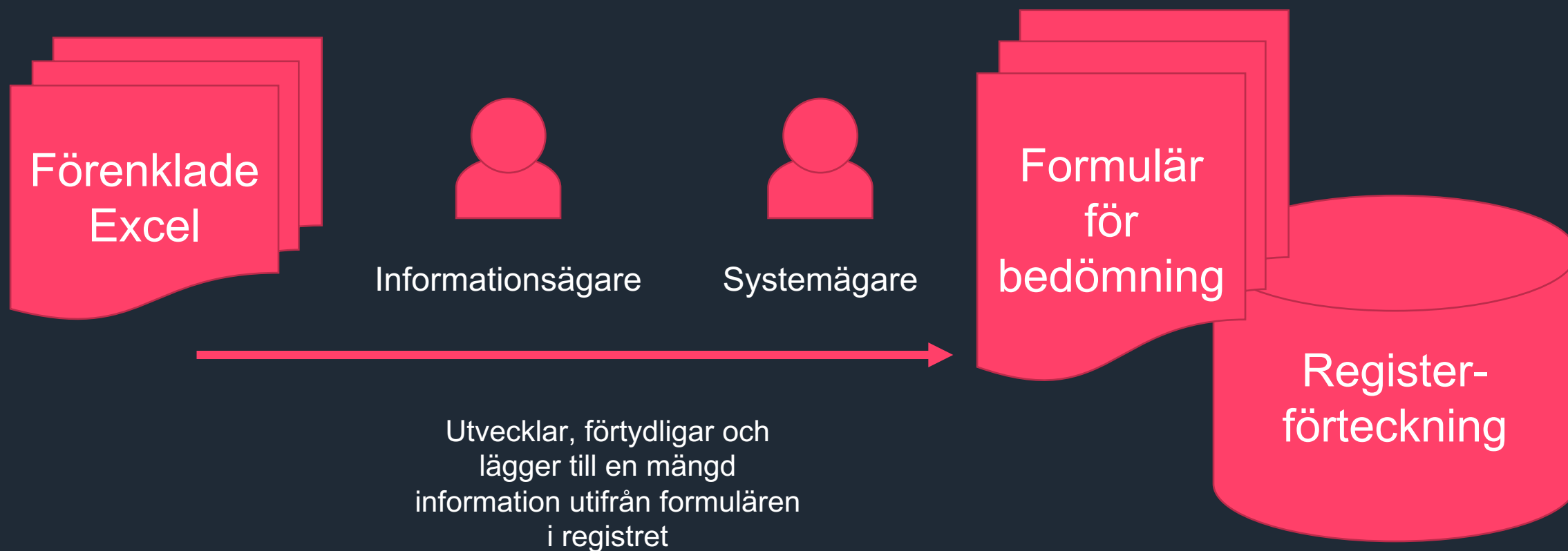
Årshjul

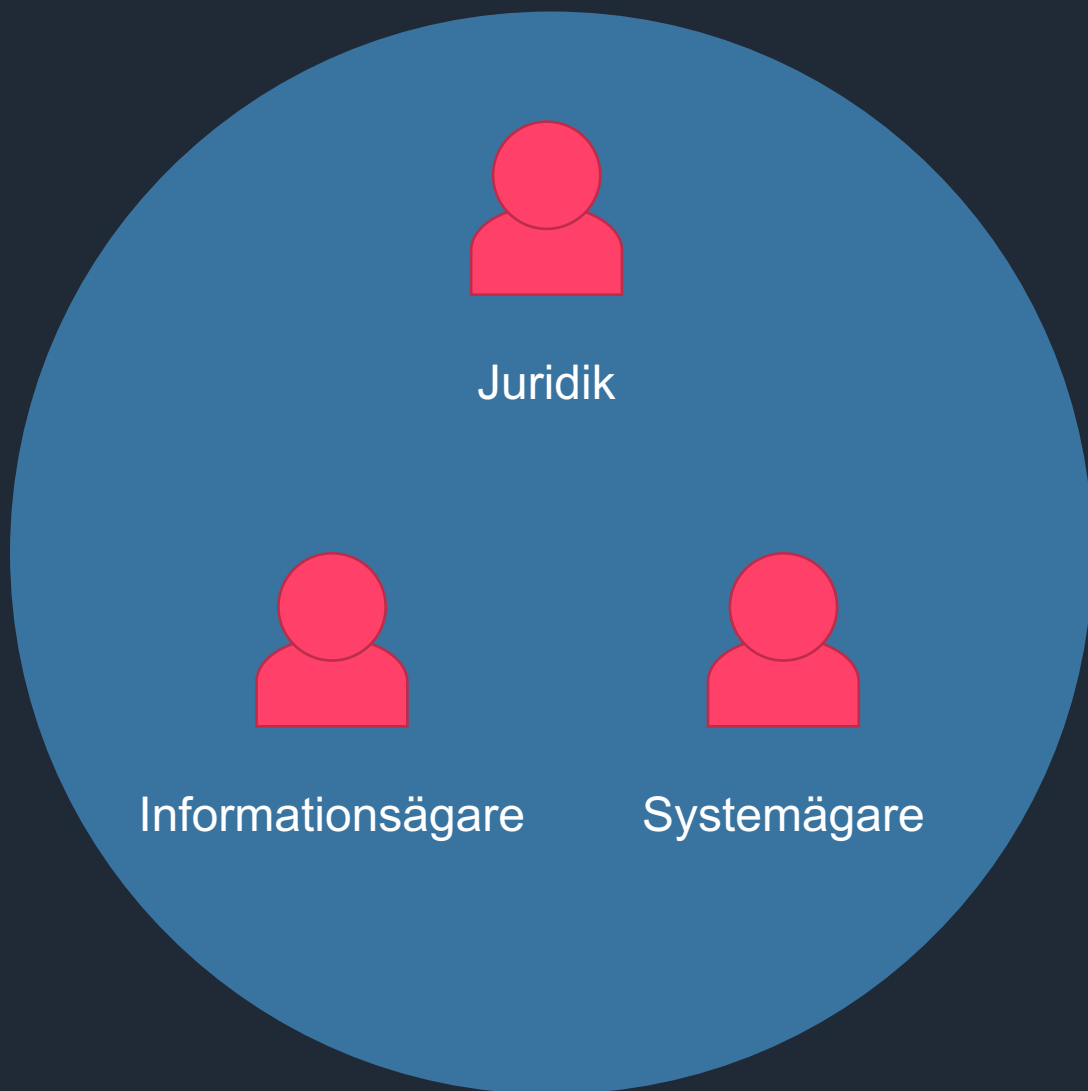


Respektive processansvarig
fyller i en förenklad excelmall

Förenklad Excel per process

- Namn (på behandlingen)
- Beskrivning
- Vems personuppgifter? (kund, anställd, leverantör...)
- Syfte
- Vilka personuppgifter?
- Vilka system?
- Hur informeras berörda?
- Laglig grund
- Gallringsrutin

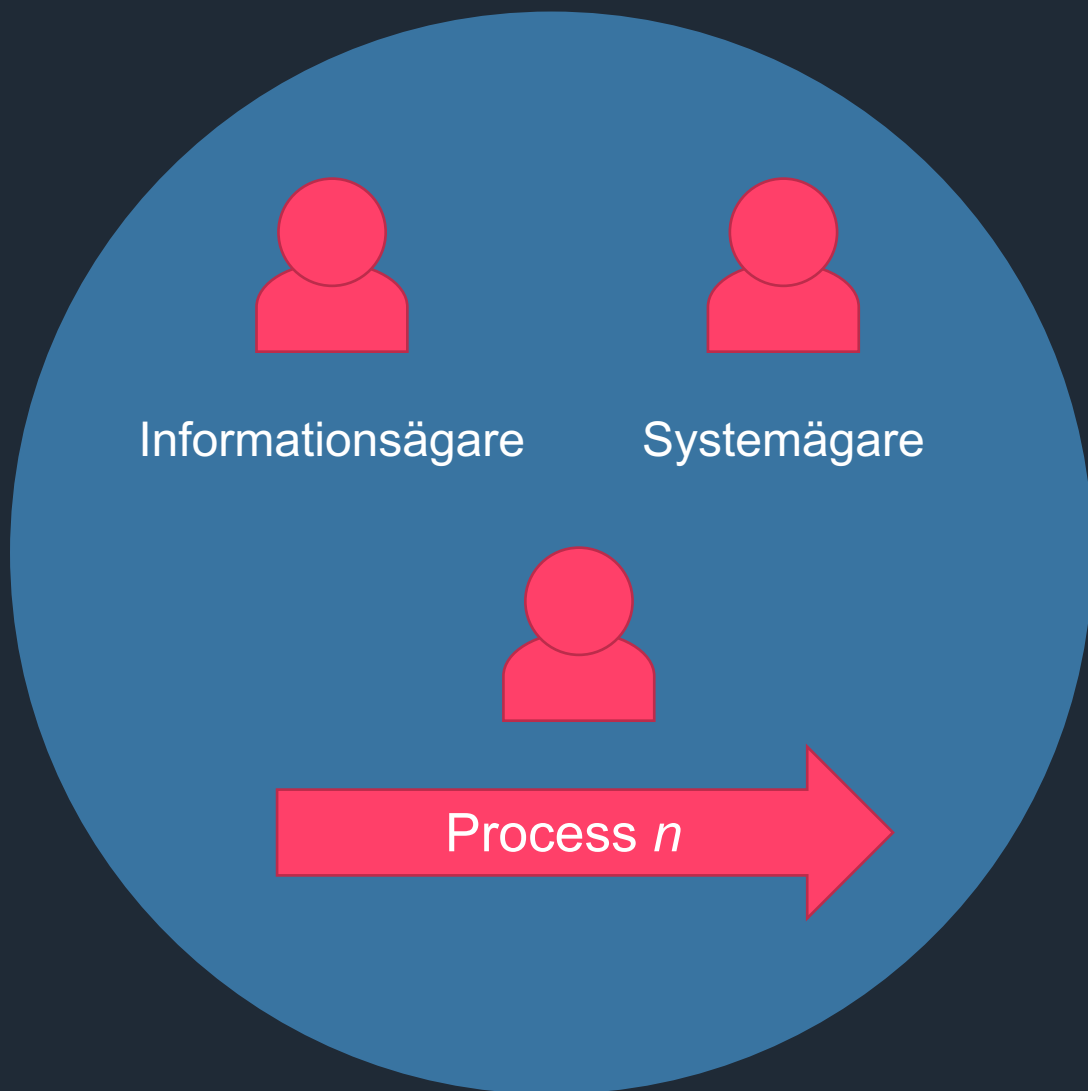




Granskar, justerar, flaggar
upp risker och
förbättringar, genomför
tröskelanalys och
godkänner.

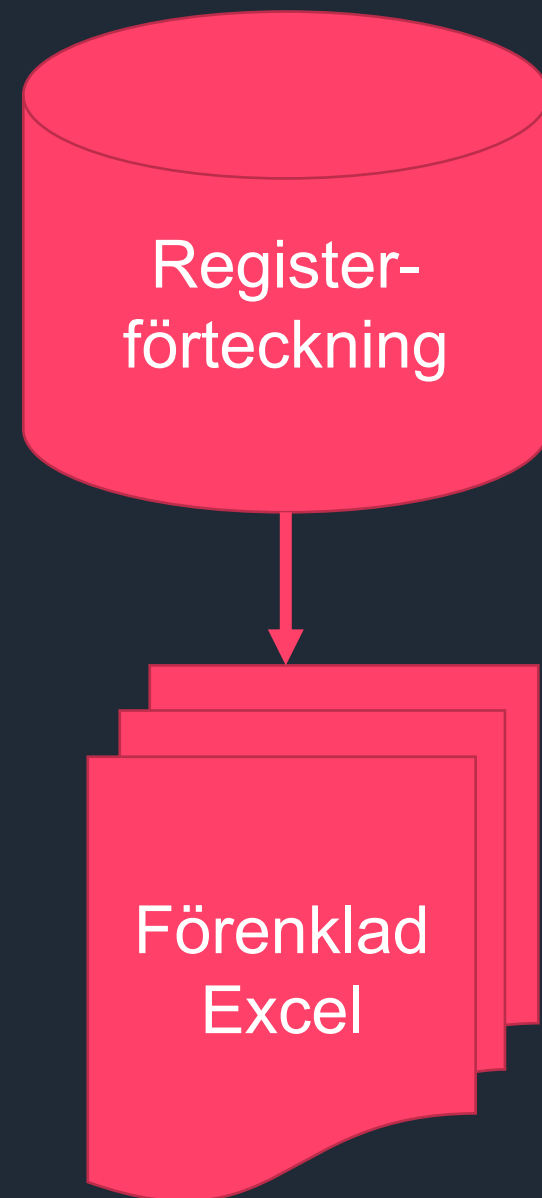
Uppgifterna i formuläret
flyttas till
registerförteckningen efter
godkännande.

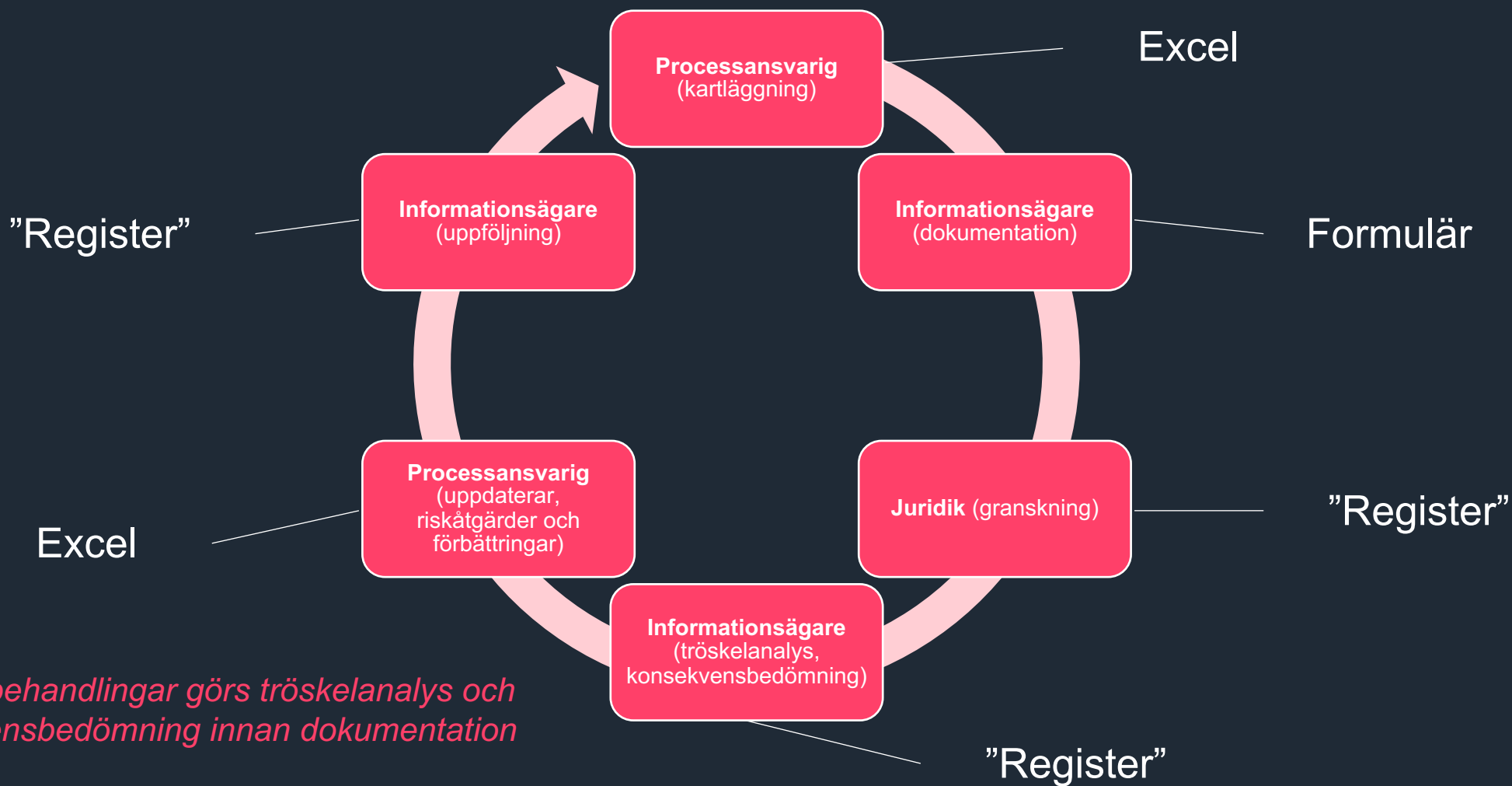




Återkopplar justeringar
och uppdaterar Excel.

Nödvändiga
konsekvensbedömningar
som identifierats vid
tröskelanalys genomförs i
processen.





Några erfarenheter och lärdomar

- Initialt mycket grupparbete vilket är resurskrävande men bidrar till lärande och underlättar förbättring av processen vilket förhoppningsvis innebär ett mer rutinorienterat arbete på sikt
- Redundant information i Excel och register innebär merarbete men det möjliggör en relativt effektiv arbetsfördelning
- Att redan från början upprätta en "fullständig" dokumentation hade varit svårt utan stödet från juridikavdelningen. Annars hade en lättare kartläggning (i nivå med Excelmallen) med uppföljande förbättringsarbete troligtvis varit en mer framkomlig väg
- Viktigt att nya personuppgiftsbehandlingar utformas så att de blir enkla och överskådliga från början
- Tydlig dokumentation är helt avgörande för att kunna förvalta personuppgiftsbehandlingar vid förändringar, tillägg, uppföljning eller revision
- Positivt bidrag till det övergripande informationssäkerhetsarbetet och vice versa



Tack!