transcendent group GOVERNANCE RISK COMPLIANCE

Helhetlig rammeverk for informasjonssikkerhet og personvern

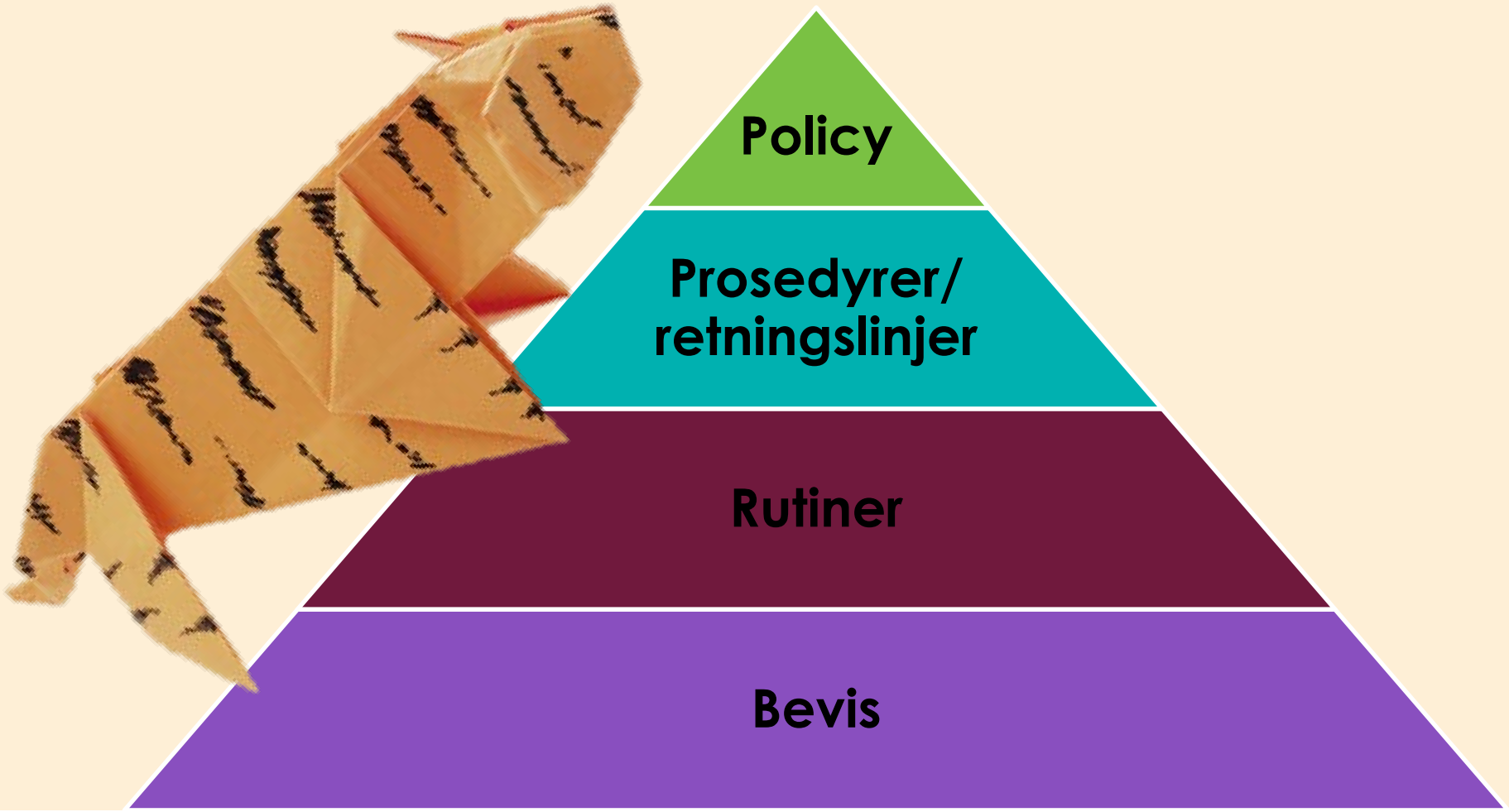
Normkonferansen

Petter Ludvig Andersen

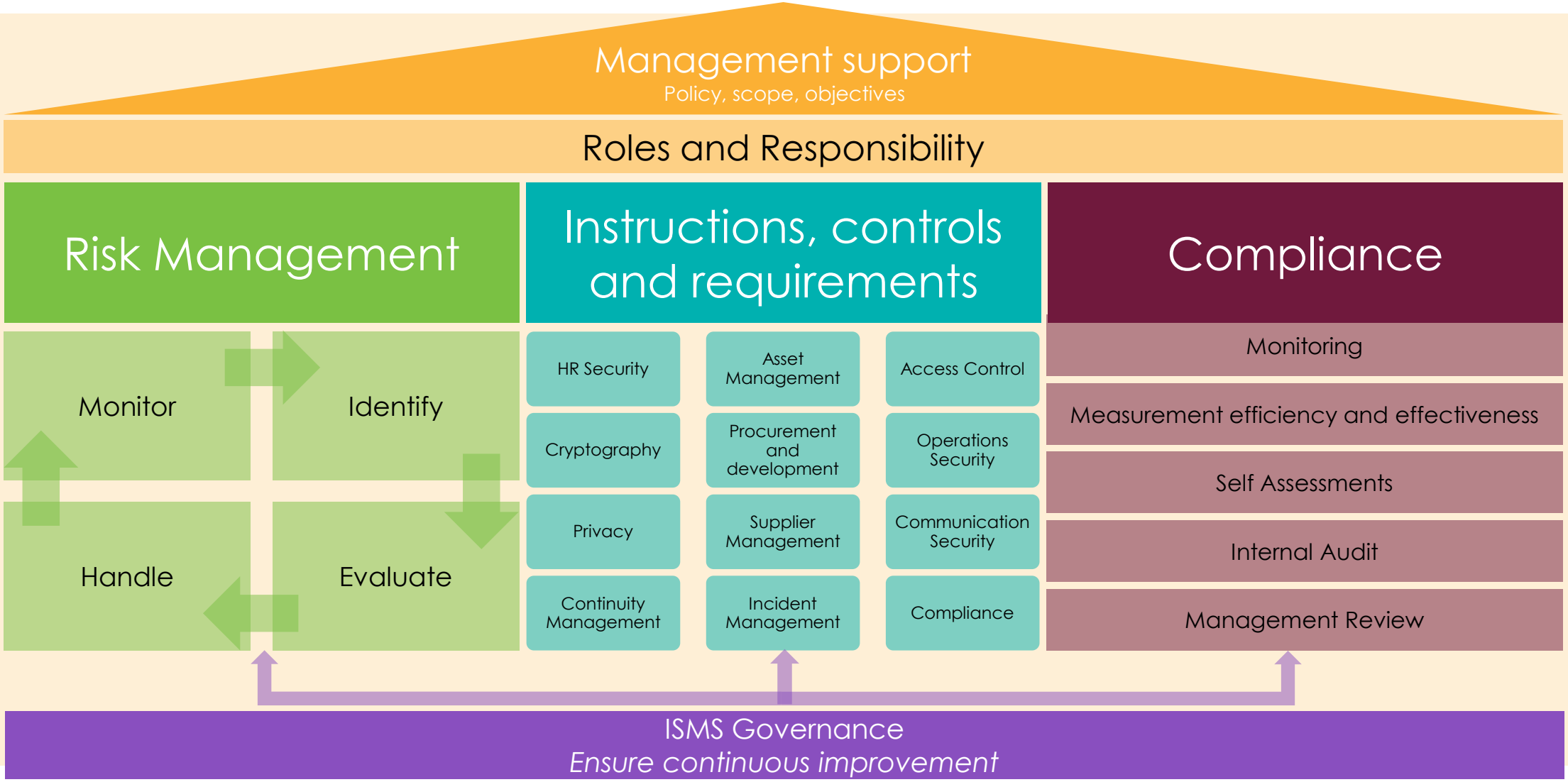
Normens (utvalgte) krav til styringssystem

- Alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern (internkontroll)
- **Informasjonssikkerhet og personvern bør inngå som en del av det totale styringssystemet i virksomheten**
- Styringssystemet skal dokumenteres

Hvordan «folk flest» ser på styringssystemer

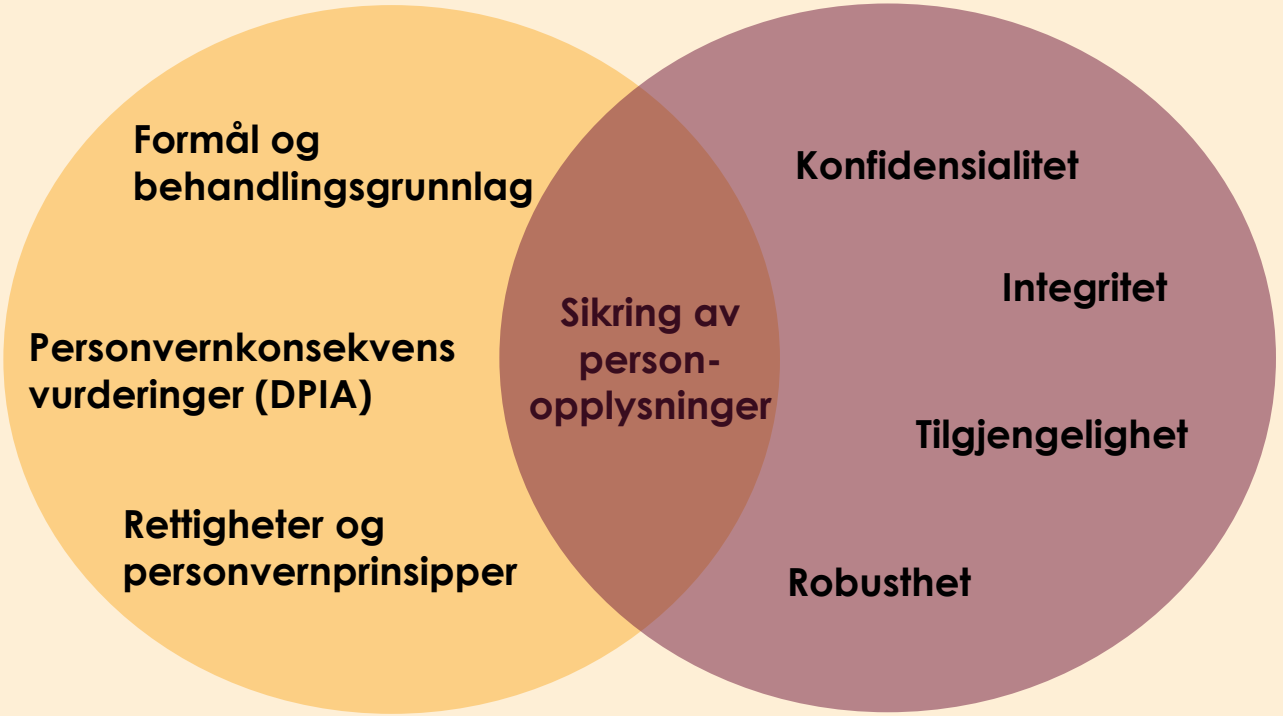


Hva styringssystemer egentlig er?



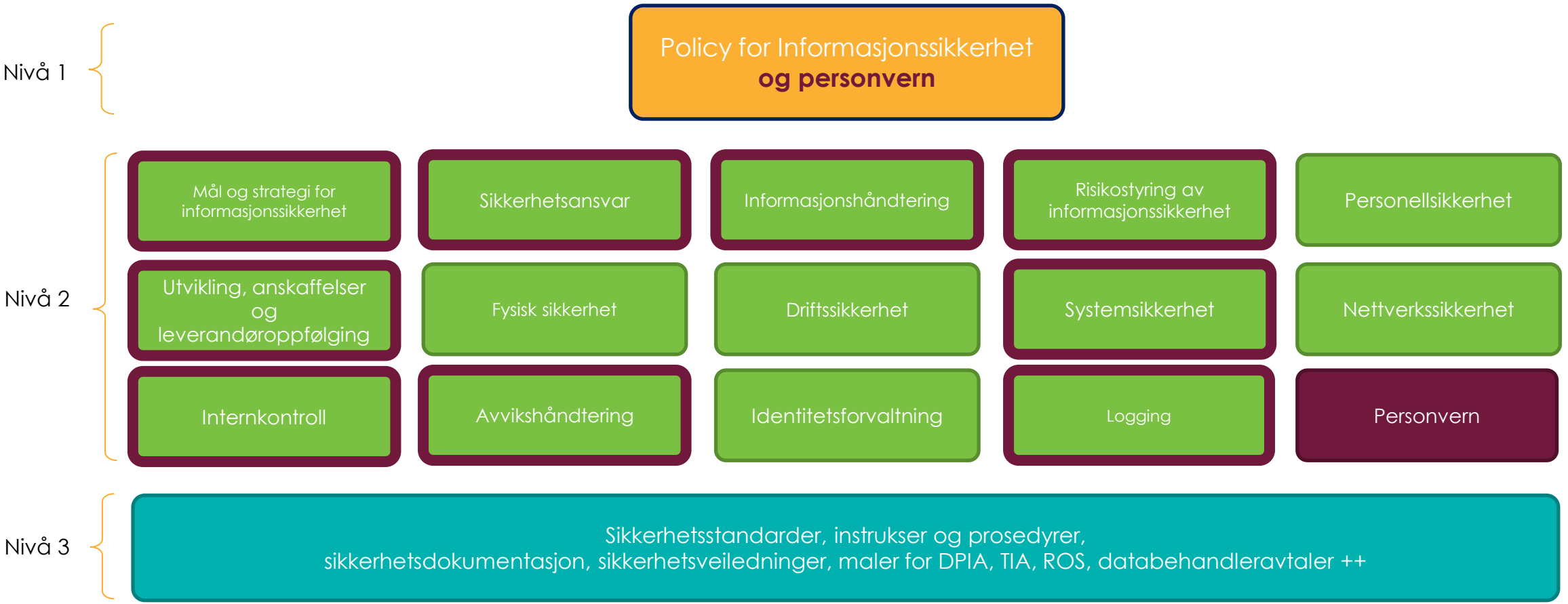
Sammenheng mellom personvern og informasjonssikkerhet

Personvern (personopplysninger)



Informasjonssikkerhet (alle typer informasjon)

Tilpasning av styringssystem for Informasjonssikkerhet

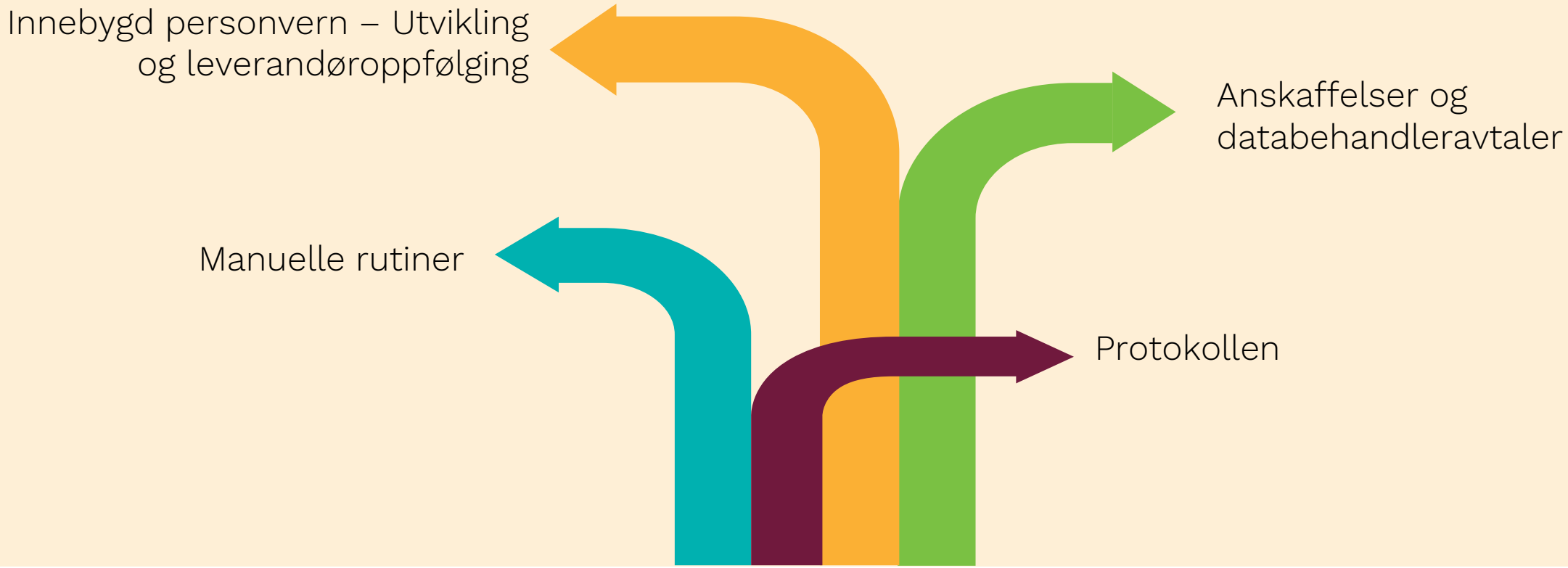


“GDPR” rutiner/prosesser/retningslinjer

- Artikkel 30 protokoll
- Ivaretakelse av personvernprinsipper
- Rutine for personvernkonsekvensvurderinger DPIA
- Risikovurdering av brudd på personopplysningssikkerheten (vurdering av melding til Datatilsyn og varsling til registrerte)
- Rutine for innsyn
- Rutine for retting og sletting
- Overføringer av personopplysninger til tredjeland / “Transfer Impact Assessments”

Prinsippet om lagringsbegrensning

Hvordan ivareta krav til sletting av personopplysninger gjennom et styringssystem?



Tilpass organisasjonen – Unngå sikkerhet og personvern på sidelinjen

1.Skreddersøm

Baser prosedyrer og krav på kunnskap om organisasjon, strategi, behov og risiko i virksomheten

2. Integrasjon

Unngå at sikkerhet og personvern blir et tillegg, og heller blir integrert i eksisterende roller, prosesser og verktøy.

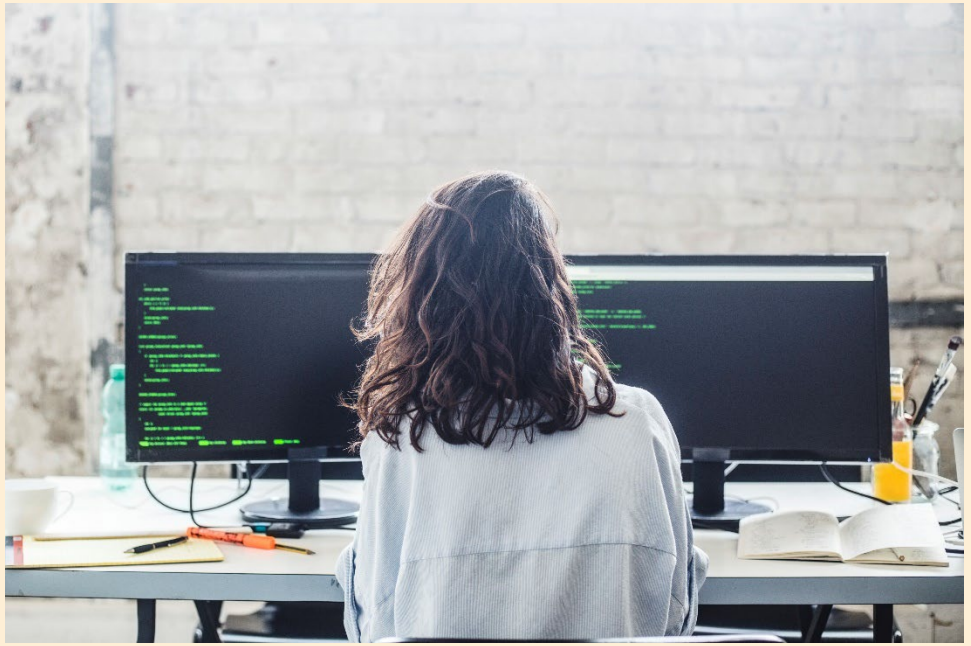
3. Gjenbruk

Bygg i størst mulig grad på eksisterende dokumentasjon og verktøy istedenfor å lage noe nytt.

Involver de rette personene.

transcendent group

Dokumentasjon ≠ dokument



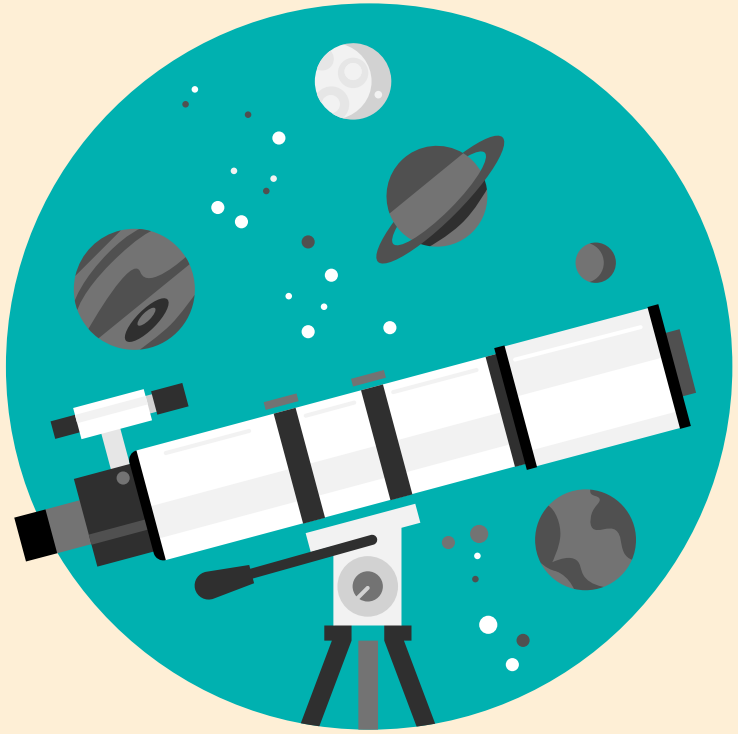
Tre nøkler til suksess

Tonen i midten

Virksomhetskultur

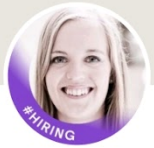
Kommunikasjon

Gode kilder til inspirasjon



- Digdir: internkontroll i praksis informasjonssikkerhet
  - Gode forklaringer, eksempler og maler
- UH-sektoren: Sikresiden.no
  - Brukervennlig og scenariobasert
- Datatilsynet:
  - innebygd personvern og personvern som standard
  - Virksomhetens plikter
- NSMs grunnprinsipper for:
  - sikkerhetsstyring
  - IKT sikkerhet
- ISMS challenges and how to solve them https://transcendentgroup.com/news/isms-challenges-and-how-you-can-solve-them/#breadcrumbs
- Normen

Spørsmål?



Eli Sofie Amdam

Teamleder i ITGS at Transcendent Group

Petter Ludvig Andersen

Personvern og informasjonssikkerhetskonsulent hos Transcendent Group