Lindahl

Presentation för Sveriges Tidskrifter om GDPR - Medlemstidskrifter

5 oktober 2017

Agenda

- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

Agenda

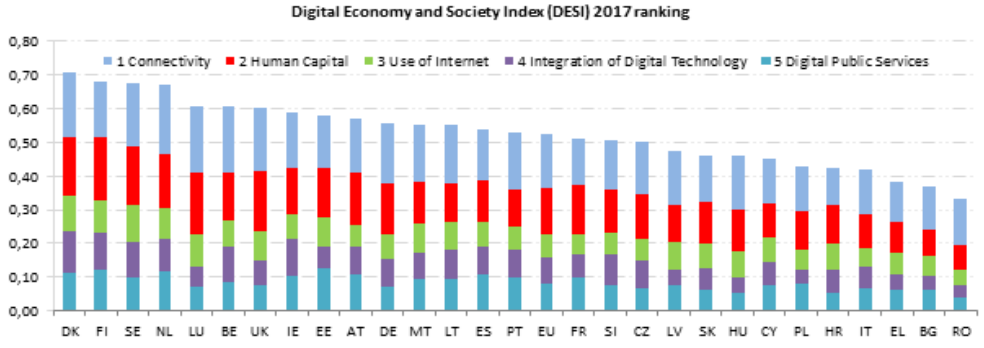
- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

GDPR – en överblick

- Träder ikraft den 25 maj 2018
- Dataskyddsdirektivet har inte givit önskad effekt
  - Föråldrad och inte anpassad till teknikutvecklingen
  - Fortsatt stor diskrepans mellan medlemsländernas implementering
- Förhoppningen med GDPR
  - Mer modernisad reglering
  - Ge individer ökad kontroll över sina personuppgifter
  - Minska diskrepansen på den inre marknaden
- Skydd mot behandling av personuppgifter är en fundamental rättighet för alla EU-medborgare

GDPR – i vilket sammanhang?

- Dataskydd och informationssäkerhet är strategiska frågor som aktivt stödjer affärsmålen.
- ”Digitalisation ready”?
- Arbeta med rätt visioner.
- Kunden/medarbetaren i centrum.



- Arbeta in dataskyddet som operativ del från början.
- Change management – många organisationer underskattar kulturella utmaningarna inför maj 2018 – kommunikation!
- Data privacy handlar om balans mellan olika intressen.
- GDPR ger verktyg och koncept att arbeta med, vi behöver dock återuppfinna transparensen.

Agenda

- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

Centrala begrepp

Personuppgifter: varje upplysning eller information som avser en identifierad eller identifierbar fysisk person, t.ex. namn, e-post, foton, bankuppgifter.

Känsliga personuppgifter: personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, uppgifter om hälsa och sexualliv, genetiska och biometriska uppgifter (t.ex. fingeravtryck)

Ändamål: personuppgifter får bara behandlas för specifikt angivna ändamål och inga därmed oförenliga ändamål, t.ex. administration av medlemsavtal eller kundanpassad direktmarknadsföring.

Behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, t.ex. insamling, lagring, bearbetning eller ändring, läsning, utlämning genom överföring och radering.

Laglig grund: en behandling är endast laglig om behandlingen sker med stöd av en (i GDPR) utpekad grund, t.ex. samtycke, fullgörande av avtal, intresseavvägning eller fullgörande av en rättslig skyldighet.

Centrala begrepp

Personuppgiftsansvarig: den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

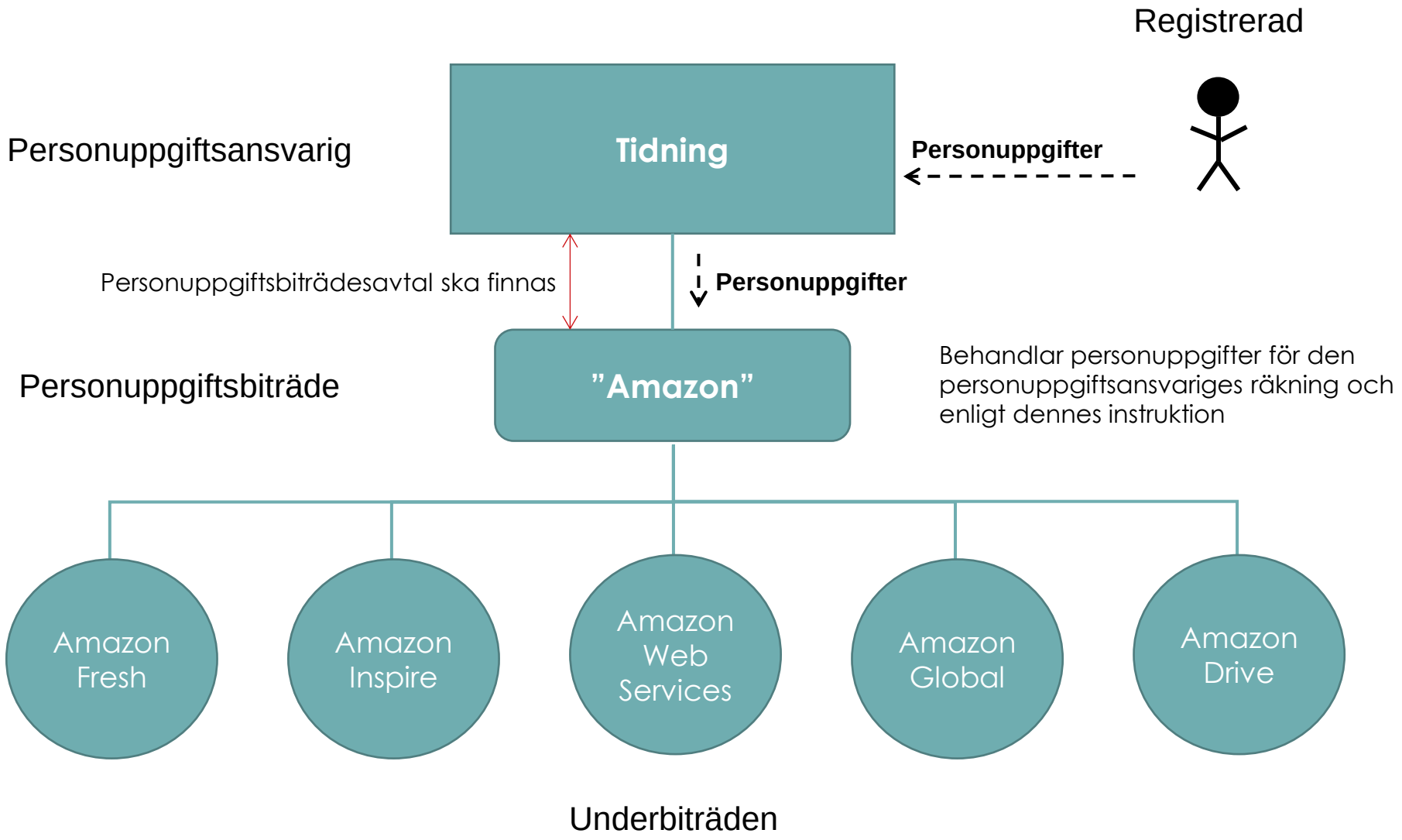
Registrerad: den fysiska person som den personuppgiftsansvarige behandlar personuppgifter om.

Personuppgiftsbiträde: den som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. en molntjänstleverantör som Amazon.

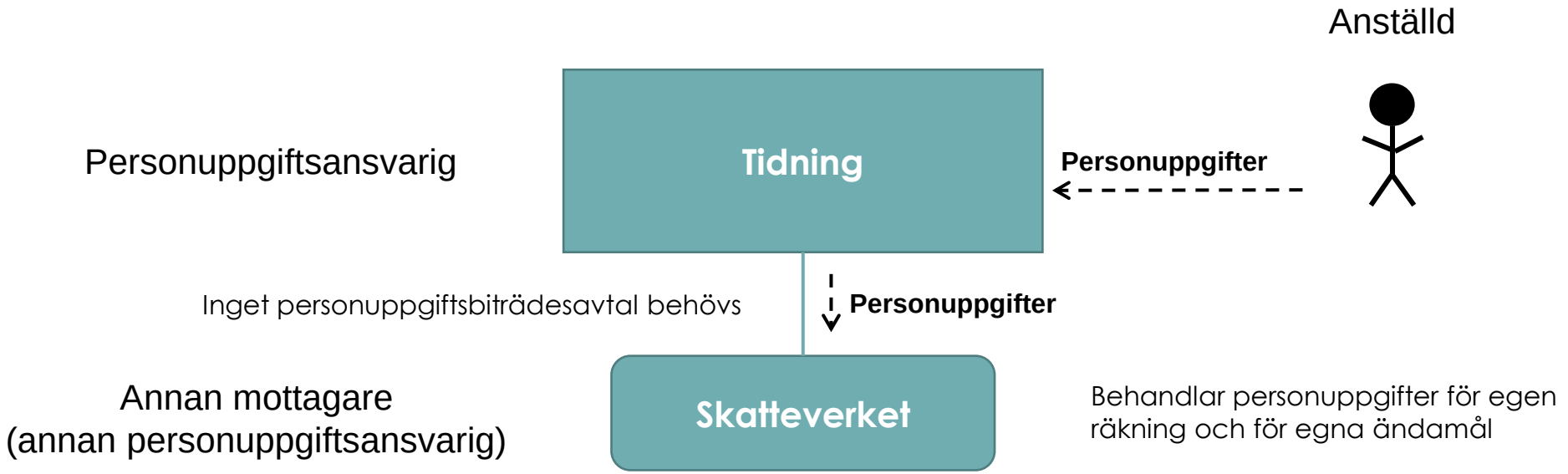
Underbiträde: den som behandlar personuppgifter för den personuppgiftsansvariges räkning på uppdrag av den personuppgiftsansvariges personuppgiftsbiträde, t.ex. en underleverantör till personuppgiftsbiträdet.

Annan mottagare: en annan part som den personuppgiftsansvarige lämnar uppgifter till och som behandlar personuppgifter för sin egen räkning, t.ex. Skatteverket och marknadsanalysbolag.

Centrala begrepp



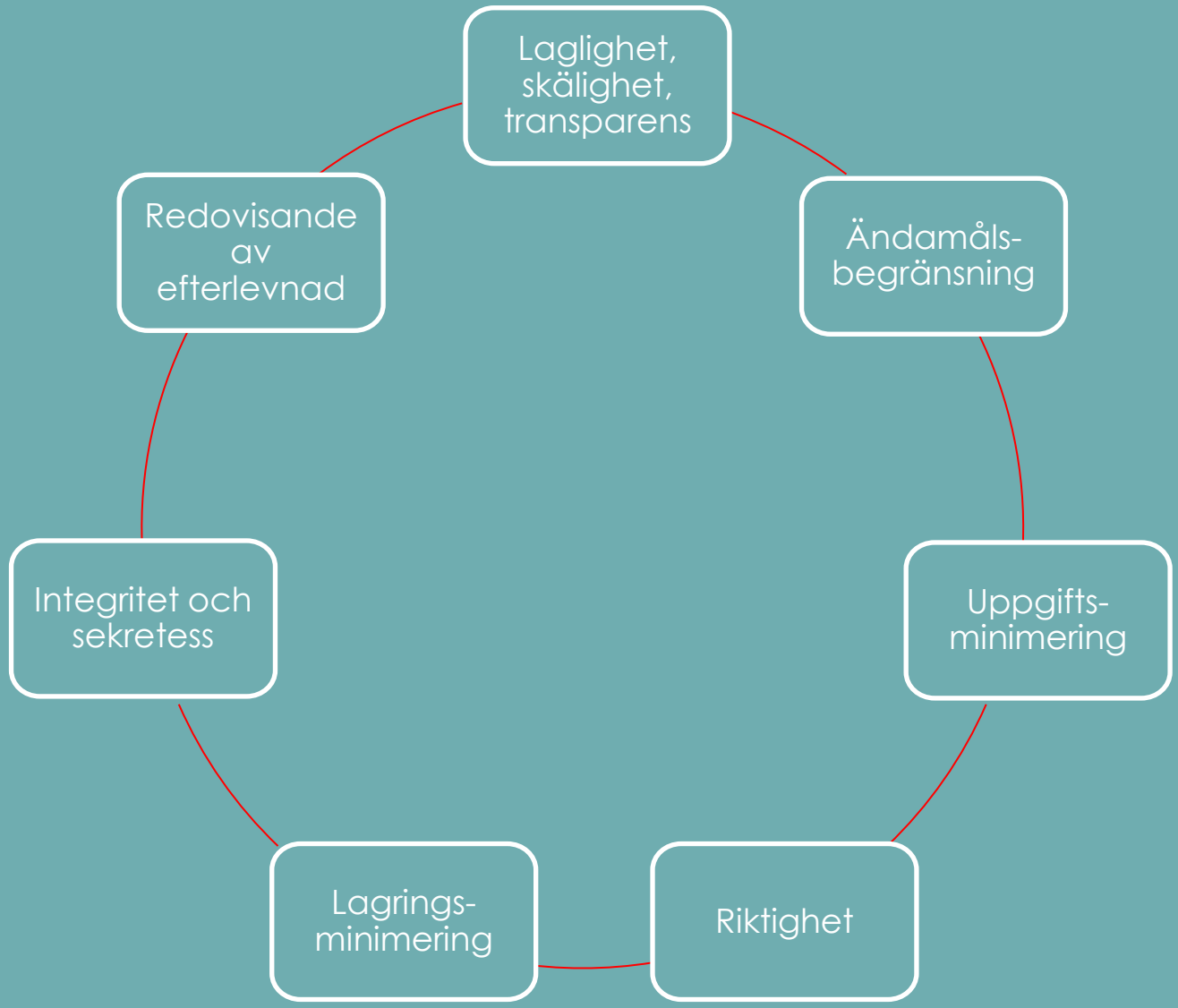
Centrala begrepp



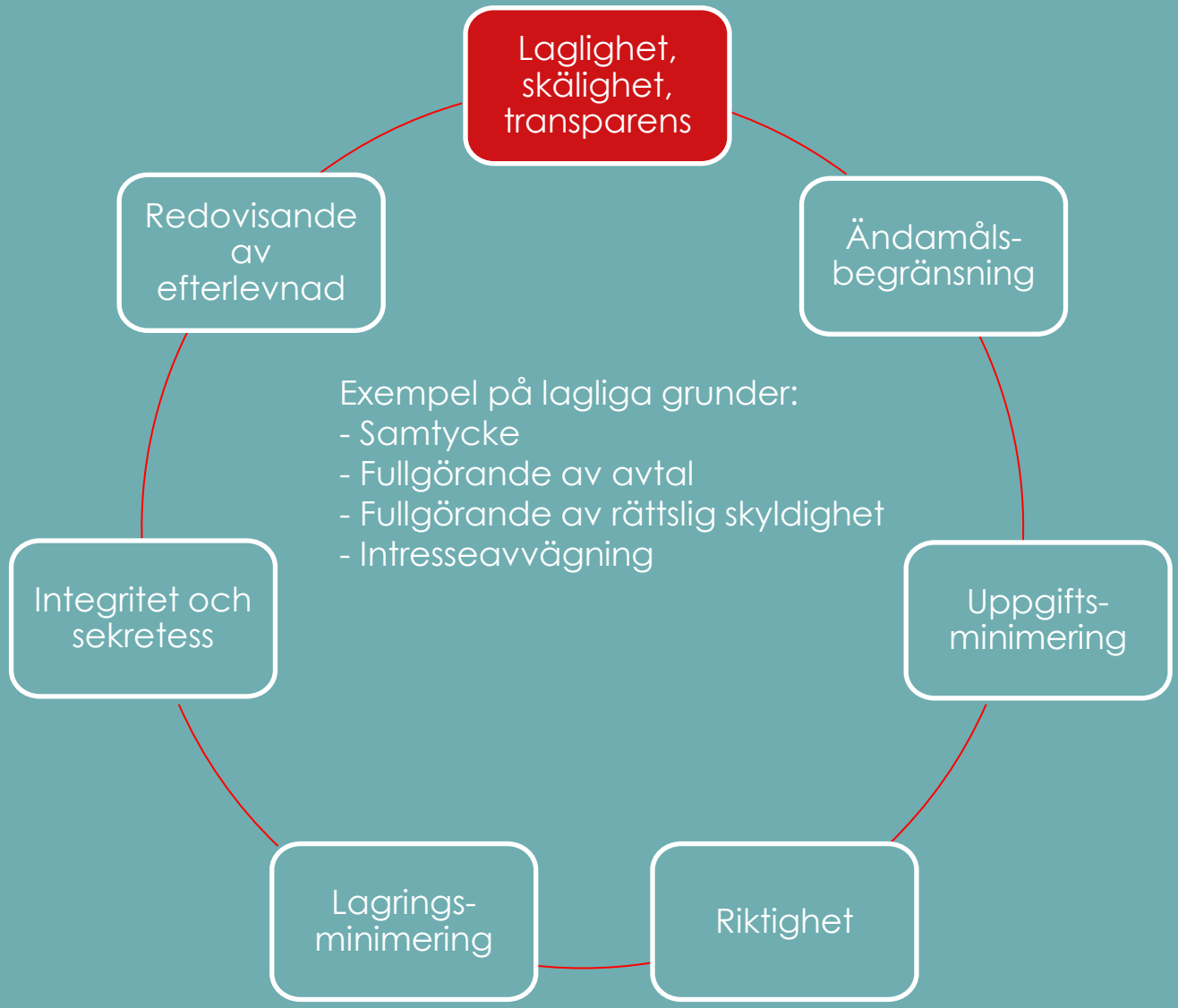
Agenda

- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

Grundläggande principer

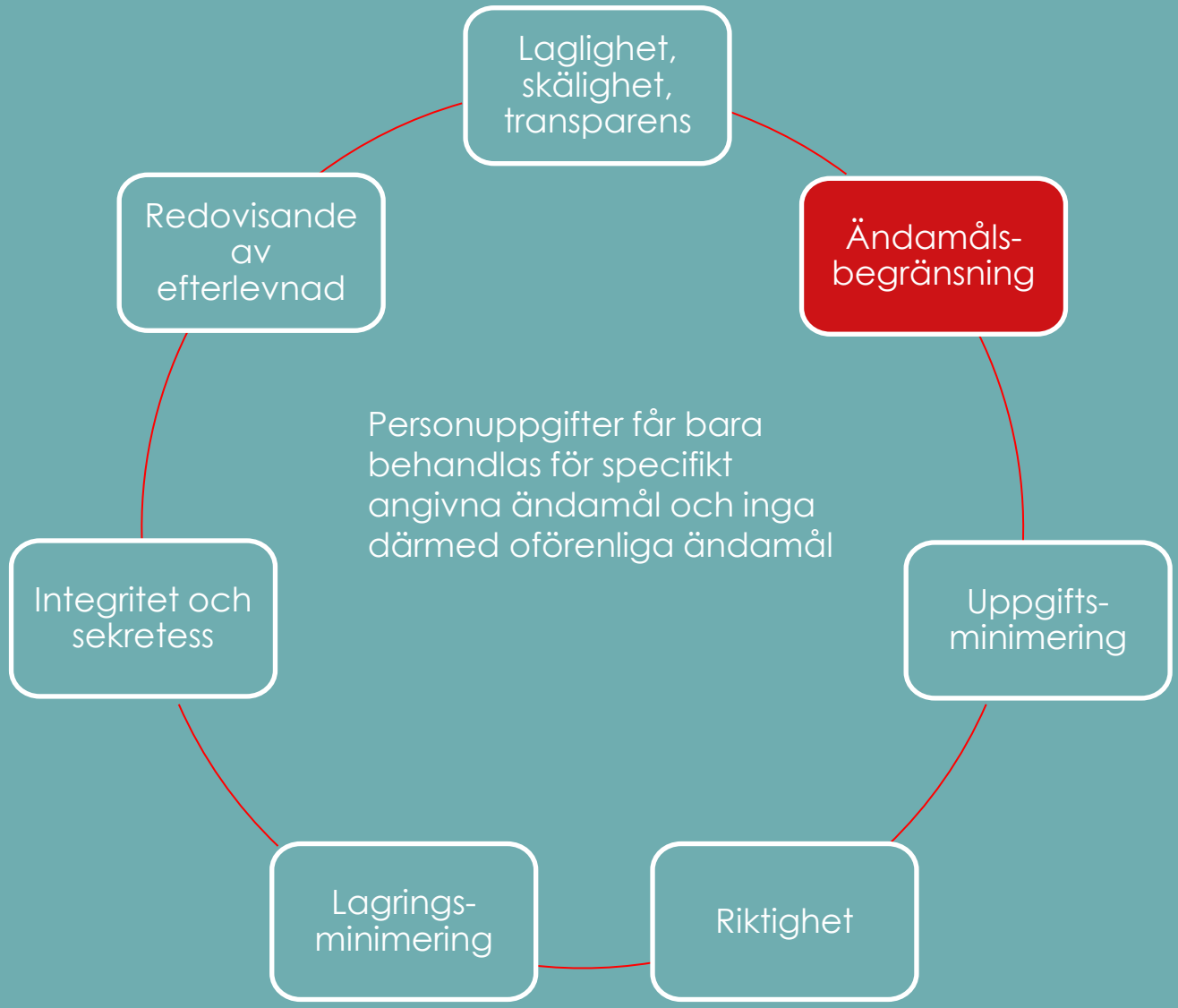


Grundläggande principer

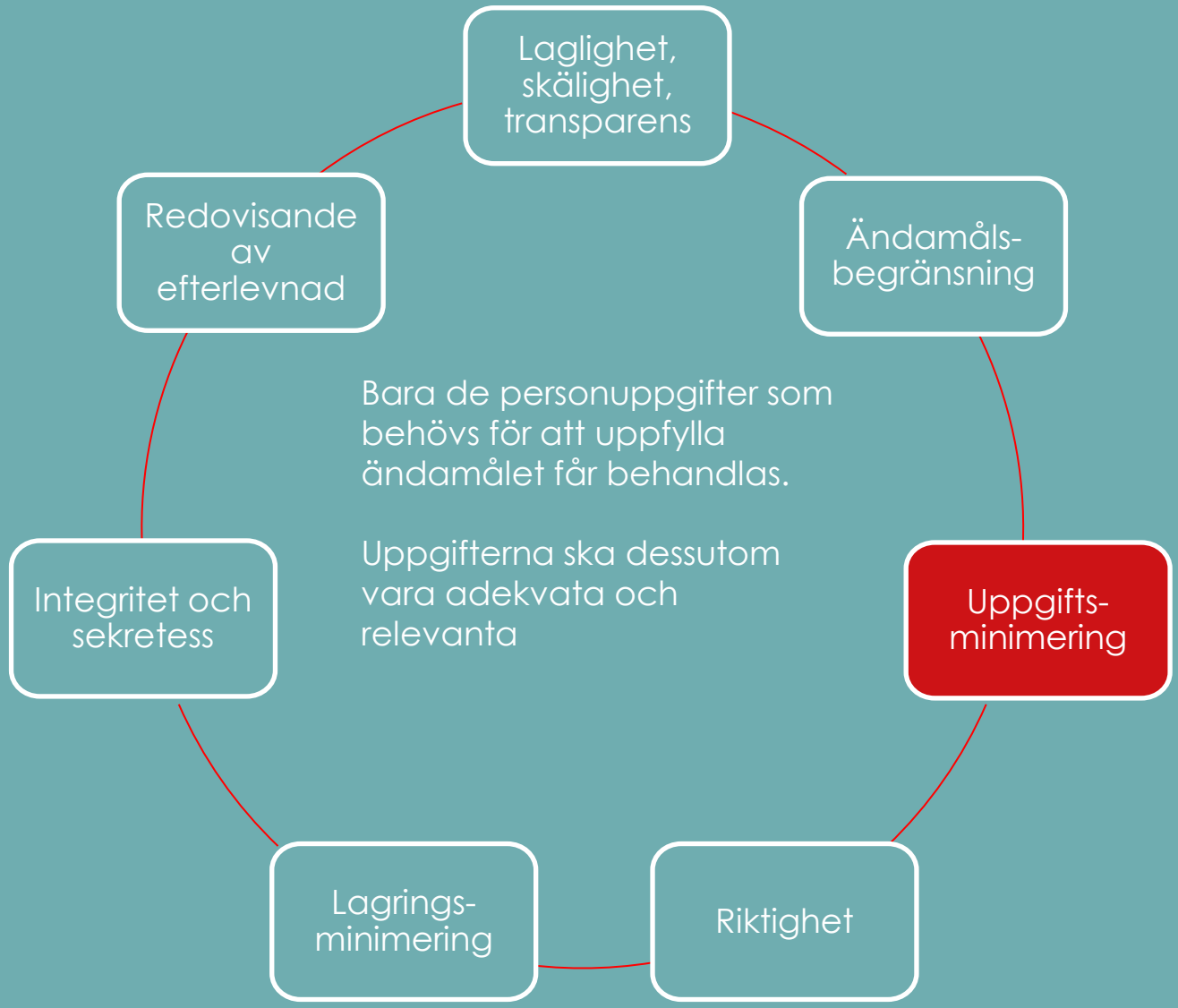


Grundläggande principer

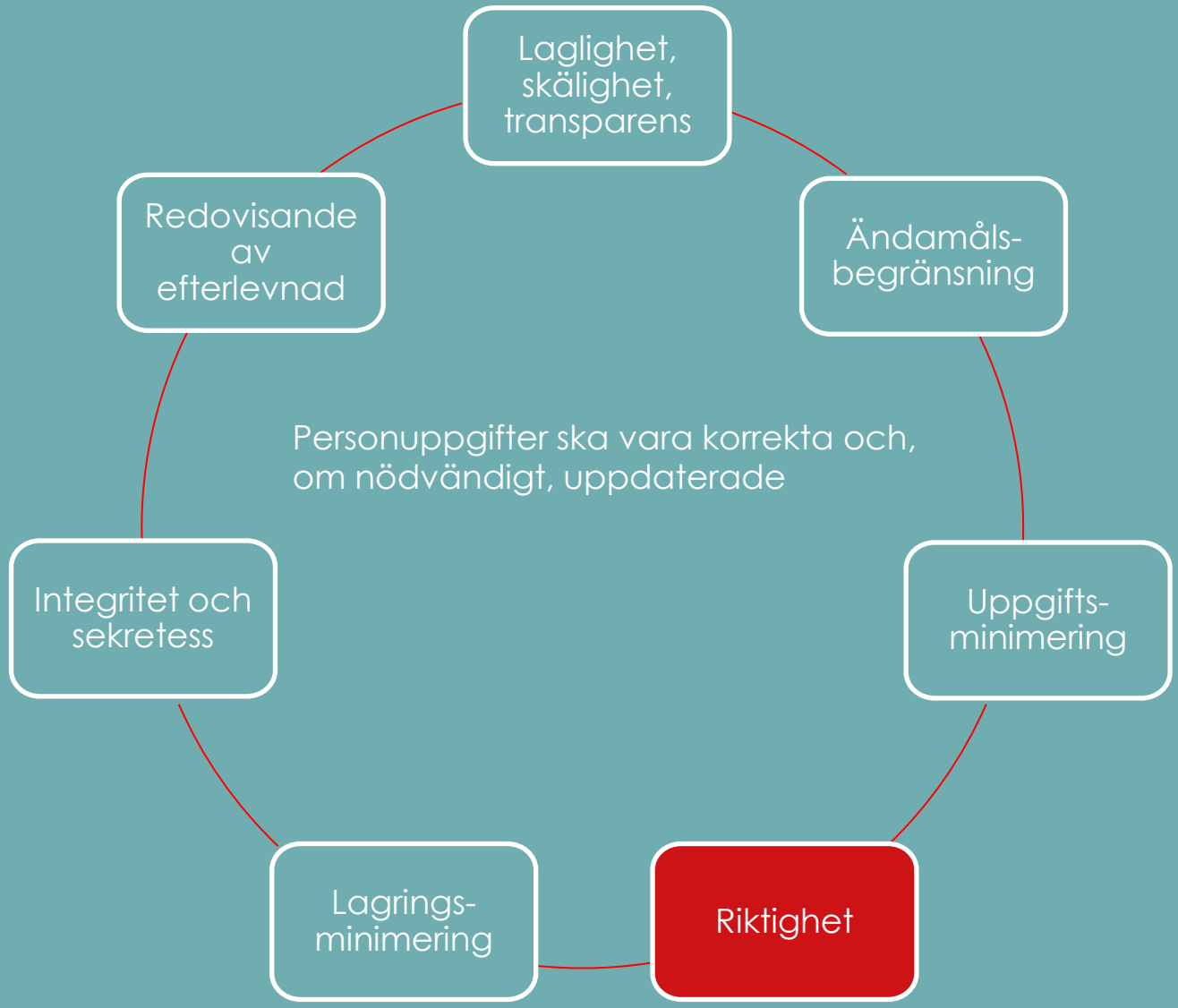
Grundläggande principer



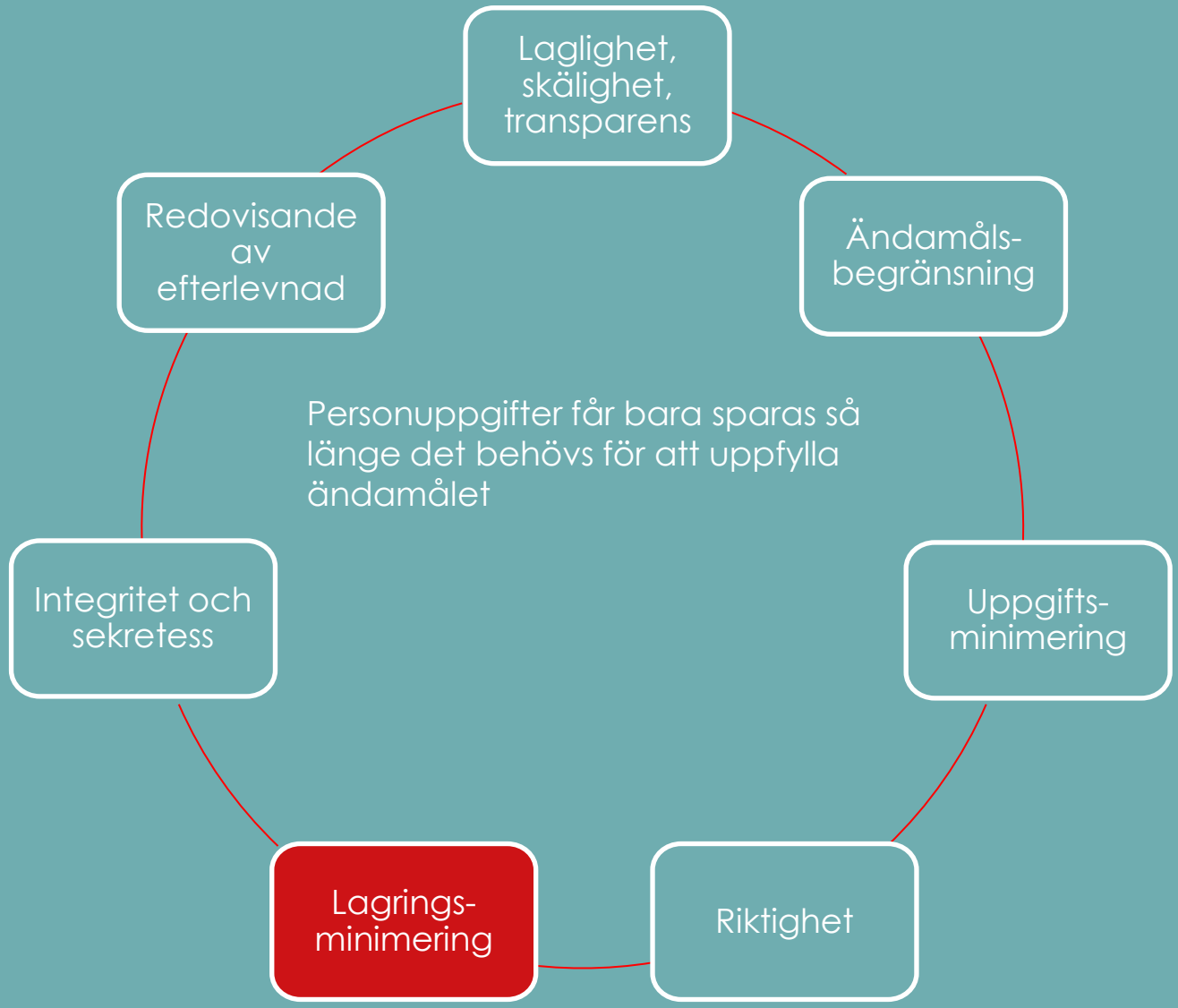
Grundläggande principer



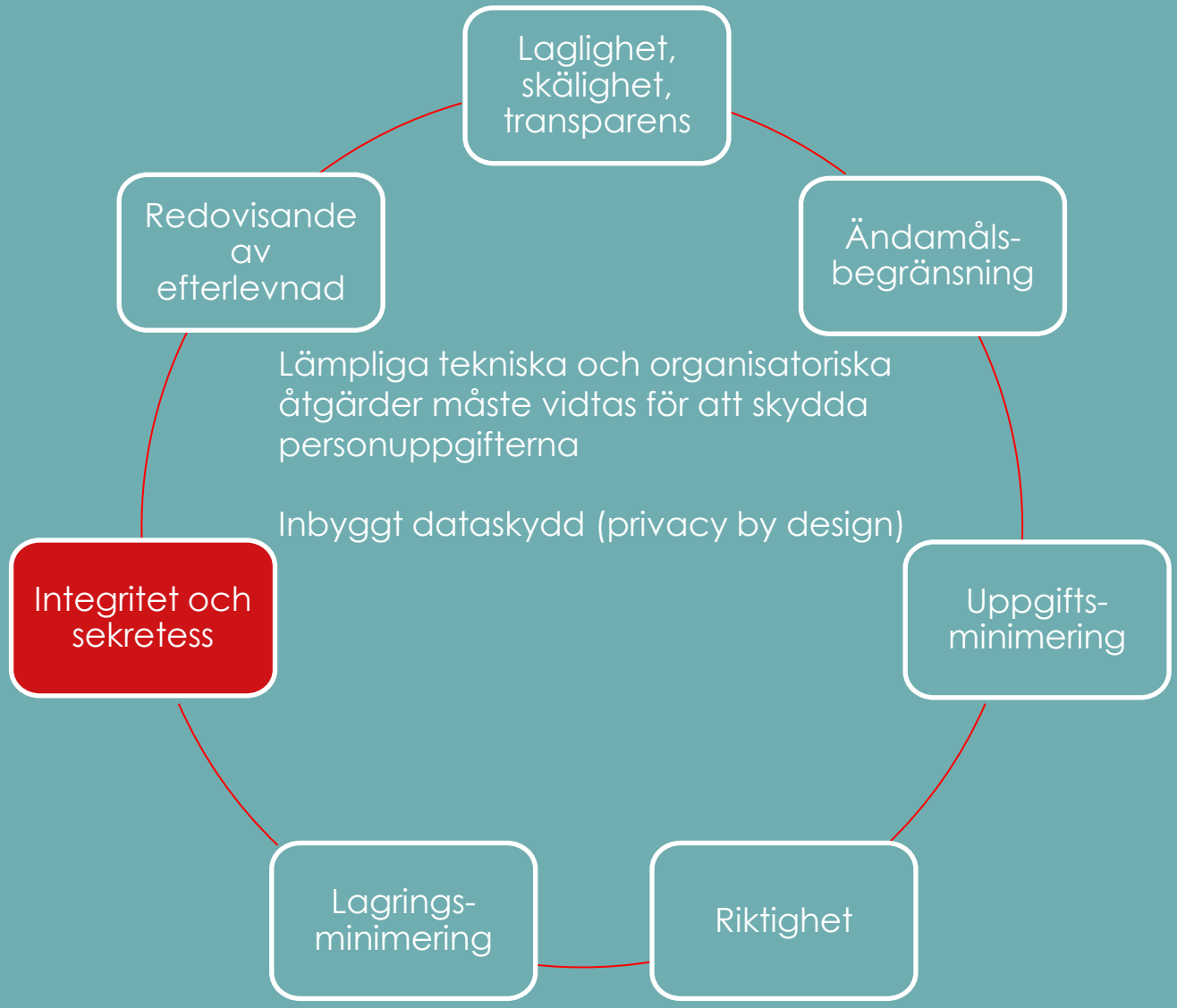
Grundläggande principer



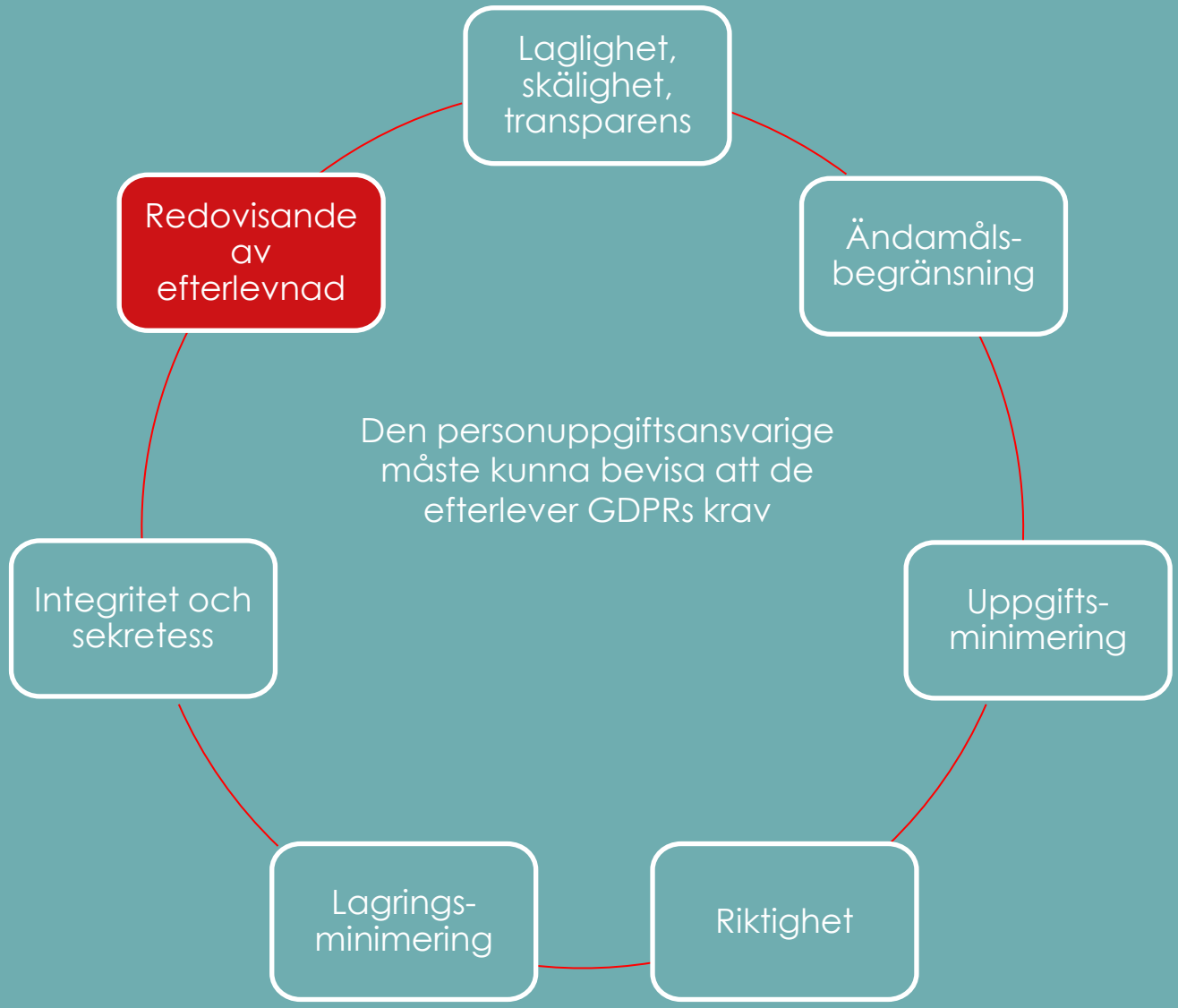
Grundläggande principer



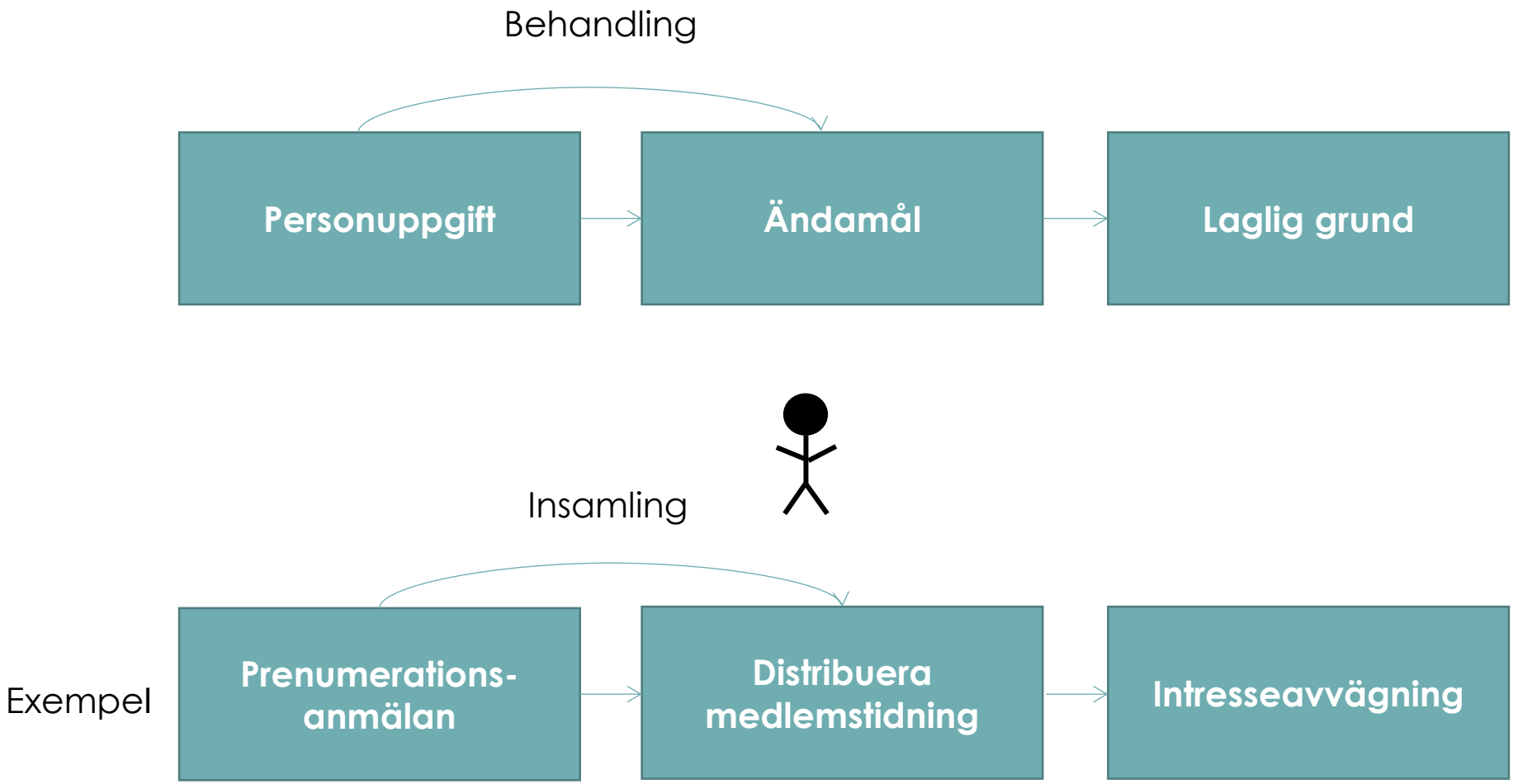
Grundläggande principer



Grundläggande principer



Grundläggande principer



Agenda

- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

GDPR i 10 punkter

1. Börjar tillämpas den 25 maj 2018

2. En förordning är direkt tillämplig – behöver inte att implementeras som svensk lag

3. Personuppgiftslagen kommer att avskaffas

4. Inga undantag för ostrukturerad behandling av personuppgifter

5. Krav på register över behandlingen av personuppgifter

6. Ökade krav på dokumentation och administration för att kunna säkerställa kontroll och visa efterlevnad (”accountability principle”)

GDPR i 10 punkter

7. Krav på utformningen av IT-system, rutiner och arbetssätt genom principerna för privacy by design och privacy by default

8. Förstärkta rättigheter för registrerade

- Ytterligare information
- Rätten att bli glömd
- Dataportbilitet m.m.

9. Krav på rapportering avseende personuppgiftsincidenter

- Till Datainspektionen inom 72 timmar
- Till registrerade utan onödigt dröjsmål

10. Kraftiga sanktionsavgifter

- Upp till det högre av 20 MEUR eller 4 % av den globala årsomsättningen

Frågor inför dataskyddsförordningens införande

- **Vem är ansvarig för organisationens dataskyddsfrågor?**
- **Vilka personuppgifter hanteras inom organisationen? Hur / till vem?**
- **Används missbruksregeln idag?**
- **Vilken information lämnas ut från organisationen?**
- **Vilka rutiner behövs för att säkerställa de registrerades rättigheter?**
- **Vilket rättsligt stöd finns för hanteringen av personuppgifter inom organisationen?**
- **Hur inhämtas samtycke?**
- **Behandlas personuppgifter om barn?**
- **Finns det särskilda integritetsrisker med behandlingen?**
- **Vilka rutiner finns för personuppgiftsincidenter?**
- **Finns skydd för personuppgifter integrerat i organisationens IT-system?**
- ***Vilka resurser krävs för att styra upp?***
- ***Vad betyder kraven för vår affär?***

Agenda

- GDPR – en överblick
- Centrala begrepp
- Grundläggande principer
- GDPR i 10 punkter
- Rekommenderade åtgärder

Rekommenderade åtgärder

- Gör GDPR till en styrelse- och ledningsgruppsfråga
- Inrätta en dataskyddsorganisation för att tillse efterlevnad
- Se till att rätt individer har adekvat kunskap om personuppgiftsreglerna
- Utse personuppgiftsombud eller annan ansvarig med rätt ansvar och kvalifikationer

Särskilt rörande tidskrifterna

Journalistiskt ändamål
- Förordningen påverkar inte verksamheter med utgivningsbevis
- Undantag kommer införas i lokal lagstiftning (dataskyddslagen) för behandling av uppgifter som sker för journalistiska ändamål (grundläggande principer, rättigheter – dock ej för adekvat säkerhet)

Samtycke
- Överväger 13 år för informationssamhällets tjänster

Känsliga personuppgifter kräver laglig grund samt tekniskt skydd
- Etniskt ursprung, politiska åsikter, religiös övertygelse, uppgifter om hälsa och sexualliv

Biträdesavtal
- Även inom koncern ifall medlemstidning ligger i eget bolag

Utländska tjänster/servrar
- Förbud mot överföring till tredje land utan adekvat skydd för uppgifterna

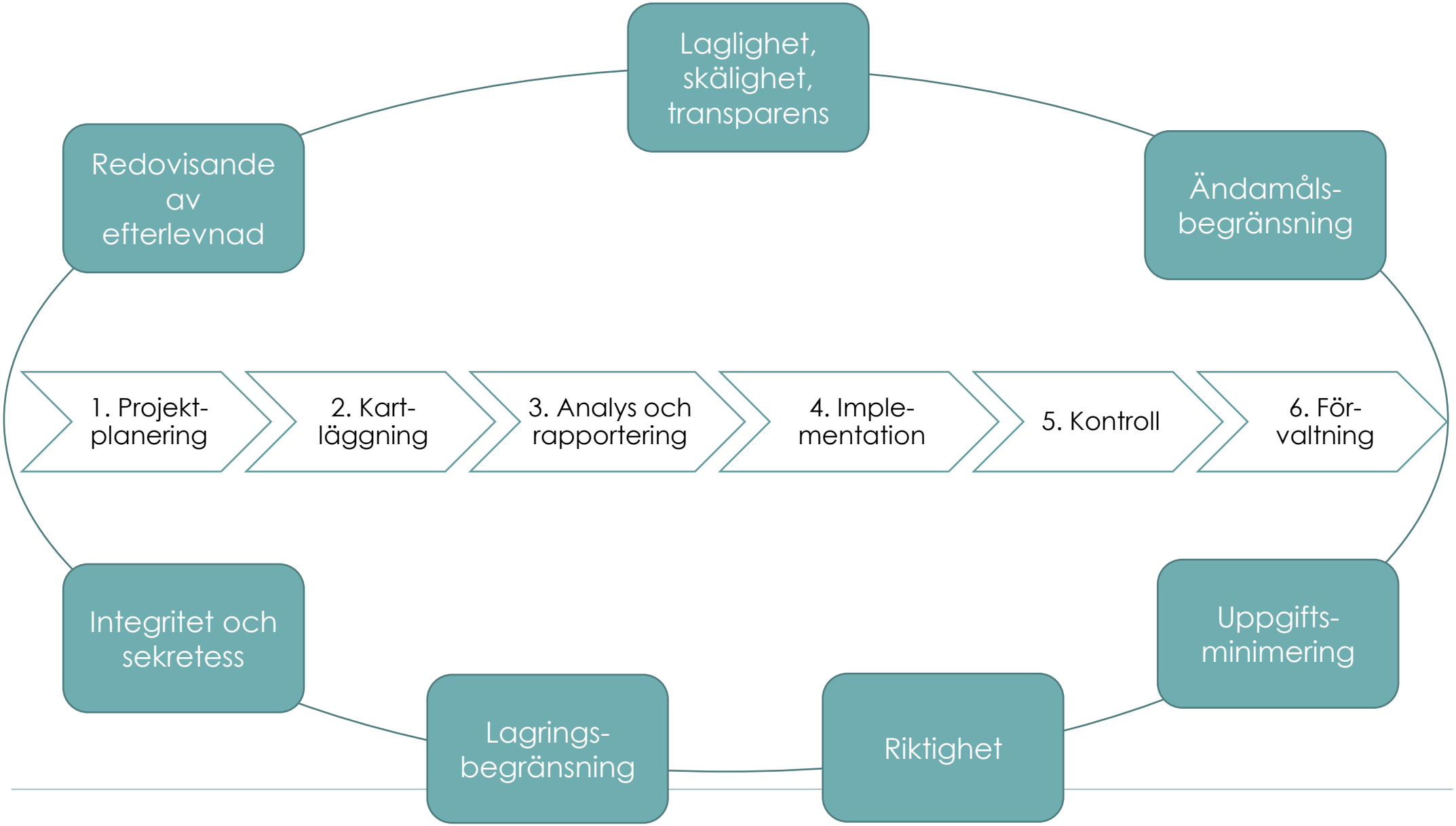
Affärsutveckling
- Stäm av syfte vid insamling, förändrad användning och laglig grund

Journalistiskt undantag
- Informera, utöva kritik och väcka debatt i samhällsfrågor
- Undantagen övriga bestämmelser, dock säkerhetskrav

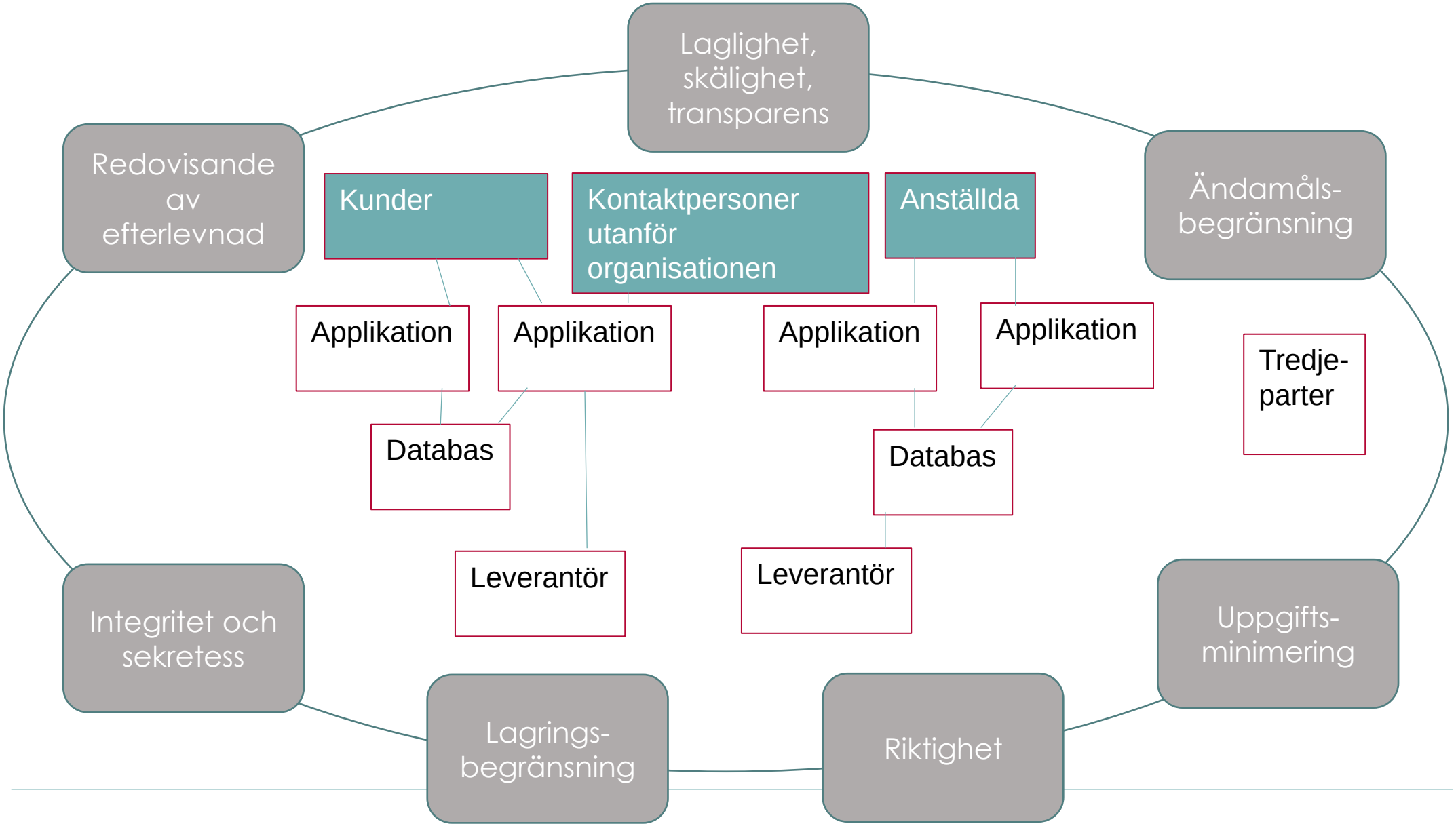
Incidenthantering
- Krav på underleverantörer, infrastruktur

Viktigt utse ansvarig för dataskydd inom varje organisation

Sex steg mot en dataskyddande organisation



Dataskyddsmodell över organisationen



Kontaktinformation

Caroline Olstedt Carlström
Delägare / Partner
070 353 90 30
caroline.olstedt.carlstrom@lindahl.se

@olstedt