KONFERENSEN
INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

17-18 SEPTEMBER 2019

GDPR – EN INTEGRERAD DEL AV INFORMATIONSSÄKERHETEN

Rose-Mharie Åhlfeldt

Bitr prof, Institutionen för Informationsteknolgi

GDPR - INGET EGET STUPRÖR!!!

- Dataskyddsförordningens krav på hantering av personuppgifter får inte bli ett eget stuprör – måste integreras med det systematiska informationssäkerhetsarbetet.

VAD ÄR INFORMATIONSSÄKERHET?

Bevarande av informationens konfidentialitet, riktighet och tillgänglighet (SS-EN ISO/IEC 27000:2018)

Säker informationshantering!!!

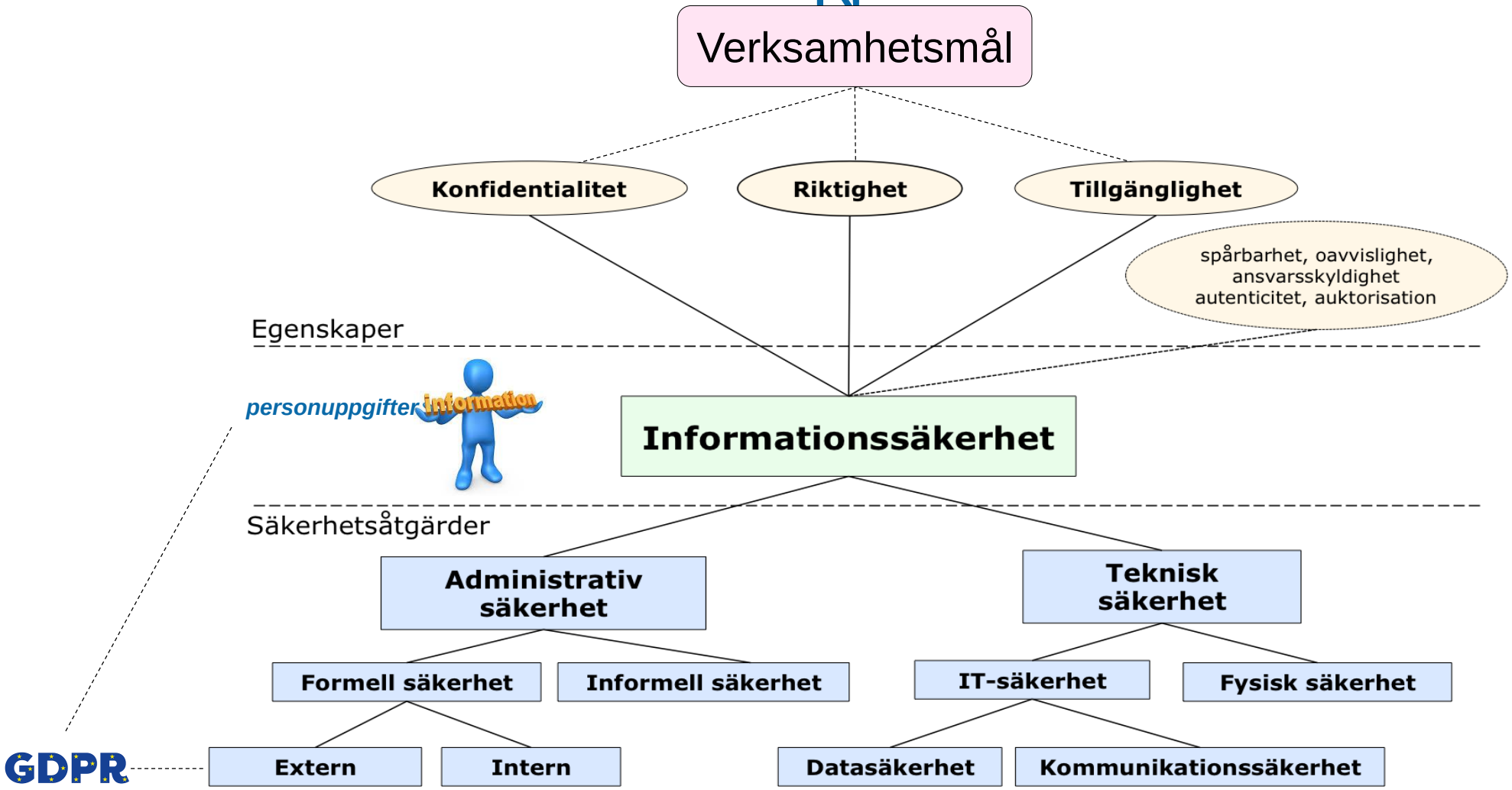
VAD ÄR INFORMATIONSSÄKERHET?

(SS-EN ISO/IEC 27000:2018)

- Informationssäkerhet inbegriper
  - tillämpning och hantering av **lämpliga säkerhetsåtgärder** som tar ett **brett spektrum av hot** i beaktande, i syfte att säkerställa organisationens verksamhet och dess **kontinuitet** samt minimera konsekvenserna av **informationssäkerhetsincidenter** .

- Informationssäkerhet uppnås
  - genom att en **lämplig uppsättning av säkerhetsåtgärder** vidtas för att skydda de identifierade **informationstillgångarna**.
  - Säkerhetsåtgärderna ska vara fastställda utifrån vald **riskhanteringsprocess** och upprätthållas **av LIS**, inbegripet policy, riktlinjer, processer, rutiner, organisationsstrukturer, mjukvara och hårdvara.
  - **Säkerhetsåtgärderna** måste specificeras, genomföras, övervakas, utvärderas och förbättras vid behov, för att säkerställa att **organisationens krav** på informationssäkerhet och **verksamhetsmål** är uppfyllda.
  - Relevanta informationssäkerhetsåtgärder förväntas vara **integrerade i organisationens verksamhetsprocesser.**

INFORMATIONSSÄKERHETSMODELLEN



SÅ … VARFÖR INFORMATIONSSÄKERHET KOPPLAT TILL GDPR?

För att **säkerställa en säkerhetsnivå som är lämplig** i förhållande till risken, inbegripet när det är lämpligt. (art 32)

- Pseudonymisering och kryptering av personuppgifter
- Förmågan att fortlöpande **säkerställa konfidentialitet, integritet (riktighet), tillgänglighet** och motståndskraft hos behandlingssystem och tjänsterna.
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en **fysisk eller teknisk incident**.
- Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de **tekniska och organisatoriska åtgärder**, som ska säkerställa behandlingens säkerhet.

DESSUTOM …

Anmälningsskyldighet vid dataintrång (art 33)

- **Incidentrapportering** till Datainspektionen inom 72 tim vid avsiktliga intrång samt oavsiktliga incidenter där personuppgifter kan läsas av obehöriga.

Konsekvensanalys (art 35)

- **Konsekvensanalys** ska vidtas vid särskilda risker med behandlingen för de registrerades fri- och rättigheter.

Förhandssamråd (art 36)

- Utökad skyldighet att samråda med Datainspektionen vid viss typ av riskfylld behandling.

SYSTEMATISK INFORMATIONSSÄKERHETSARBETE – LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

- Ett väl infört ledningssystem utifrån 27001 med till hörande säkerhetsåtgärder 27002 och vägledning 27003 står väl upp mot GDPRs krav på informationssäkerhet gällande personuppgifter.
  - Verksamhetsmål, ledning och ansvar, riskhantering och säkerhetsåtgärder.
- Personuppgifter en delmängd av informationstillgångarna.
- GDPR – en lag bland andra med krav på efterlevnad.
  - Registrerade – ytterligare en intressent med kravställningar ledningssystemet.

STANDARDER SOM GER STÖD FÖR GDPR

- **ISO/IEC 29100** – Privacy framework
  - En vägledningsstandard som beskriver och förklarar principer, terminologi och aktörer inom området privacy.
  - Kan användas för att förstå begrepp, roller och frågeställningar
  - Ingen kravstandard och kan inte användas för att visa efterlevnad av GDPR.
- **ISO/IEC 29151** – Code of practice for personally identifiable information protection.
  - Lägger till säkerhetsåtgärder till Annex A i 27001.
- **ISO/IEC 27005** – Riskhantering för informationssäkerhet
  - Relevant att lägga in DPIA i riskhanteringsprocessen
- **ISO/IEC 29134** – Privacy impact assessment – Guidelines
  - Stöd i riskhanteringsprocessen
- **ISO/IEC 27018** – Riktlinjer för skydd av personuppgifter i publika molntjänster som hanterar personuppgifter.
  - Lägger till säkerhetsåtgärder till Annex A i 27001 för molntjänster i deras egenskap av personuppgiftsbiträde.

STANDARDER UNDER UTVECKLING SOM GER STÖD FÖR GDPR

ISO/IEC 27552 – Enhancement to ISO/IEC 27001 for privacy management - Requirements

- Lägger till krav till ledningssystemet i 27001 för att hantera åtgärder och processer kring personlig integritet

ISO/IEC 29184 – Guidelines for online privacy notices and consent

- Stöder processen med att lämna information och hantera samtycke.

UTMANINGAR!!!

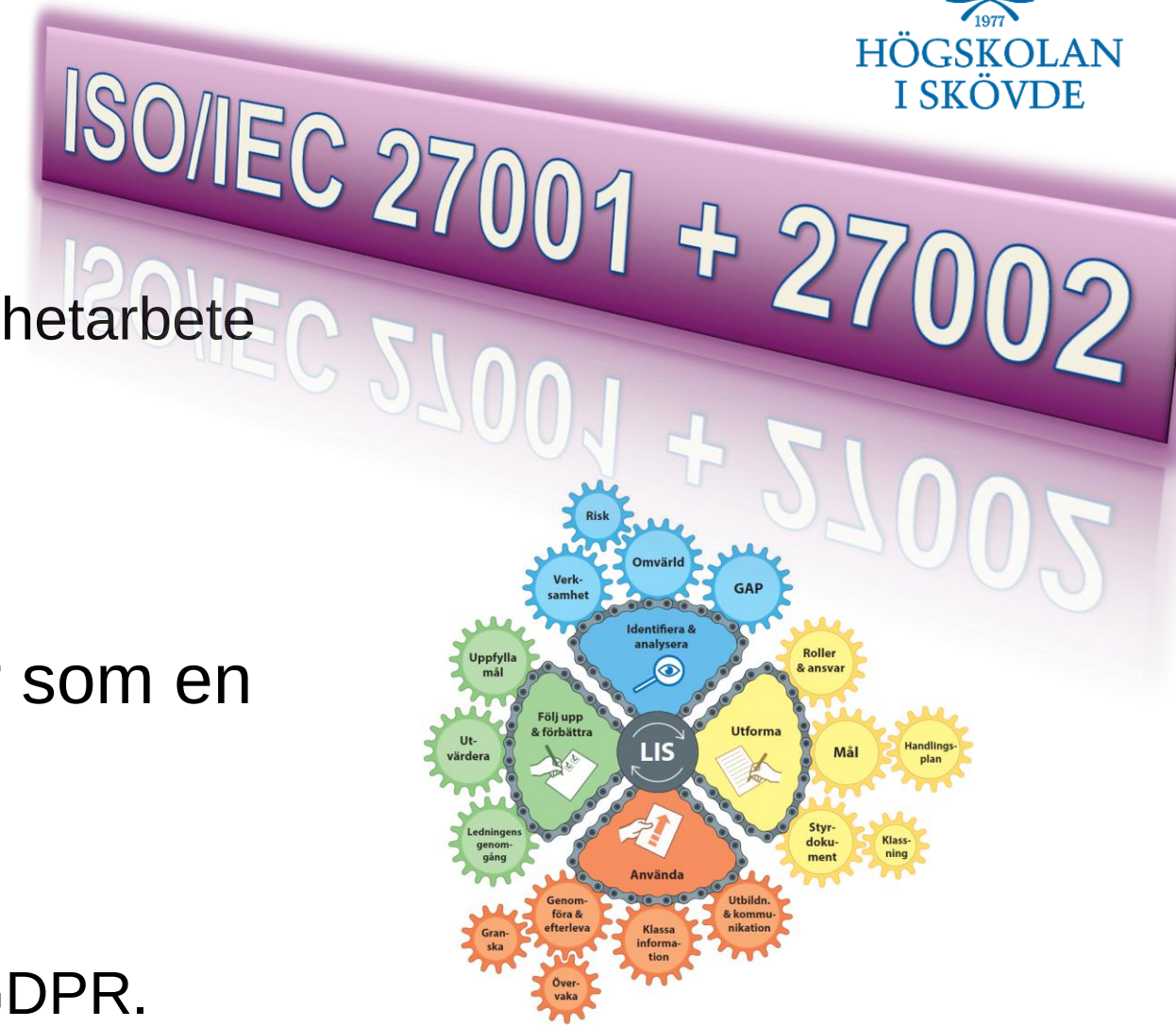
- GDPR-arbetet tagit stor kraft hos organisationer för att påbörja arbetet och åstadkomma tillräcklig efterlevnad - på bekostnad av fortsatt arbete med skyddet.
- Stort fokus på de legala aspekterna av GDPR - mindre kring fortsatt process och dagligt arbete.

UTMANINGAR!!!

- Kompetensbrist hos ledningar kring sambanden mellan GDPR och informationssäkerhet – ses ofta som två skilda områden.
- Även om informationssäkerhetsarbetet fått ett större fokus med hjälp av GDPR har det också blivit en större puckel att komma över. “ – inte ett så stort arbete till…”

HUR GÅR VI VIDARE?

- Basen finns
  - systematiskt informationssäkerhetarbete med grund från standarder
  - LIS + kompletterande privacy-standarder
  - MSBs metodstöd
- Se arbetet med personuppgifter som en del av den dagliga informationshanteringen/ informationssäkerhetsarbetet
  - inkluderat specifika krav från GDPR.



HUR GÅR VI VIDARE?

- Se till att organisera dataskydds- och informationssäkerhetsarbete integrerat.
  - Bort med stuprörstänket
- Mer utvärdering och forskning kring arbetet med integrerat informationssäkerhetsarbete
  - GDPR men även övriga områden