Integritetsskydds myndigheten

25 mars 2026

# Hantering av personuppgifter i hälso- och sjukvården – en introduktion

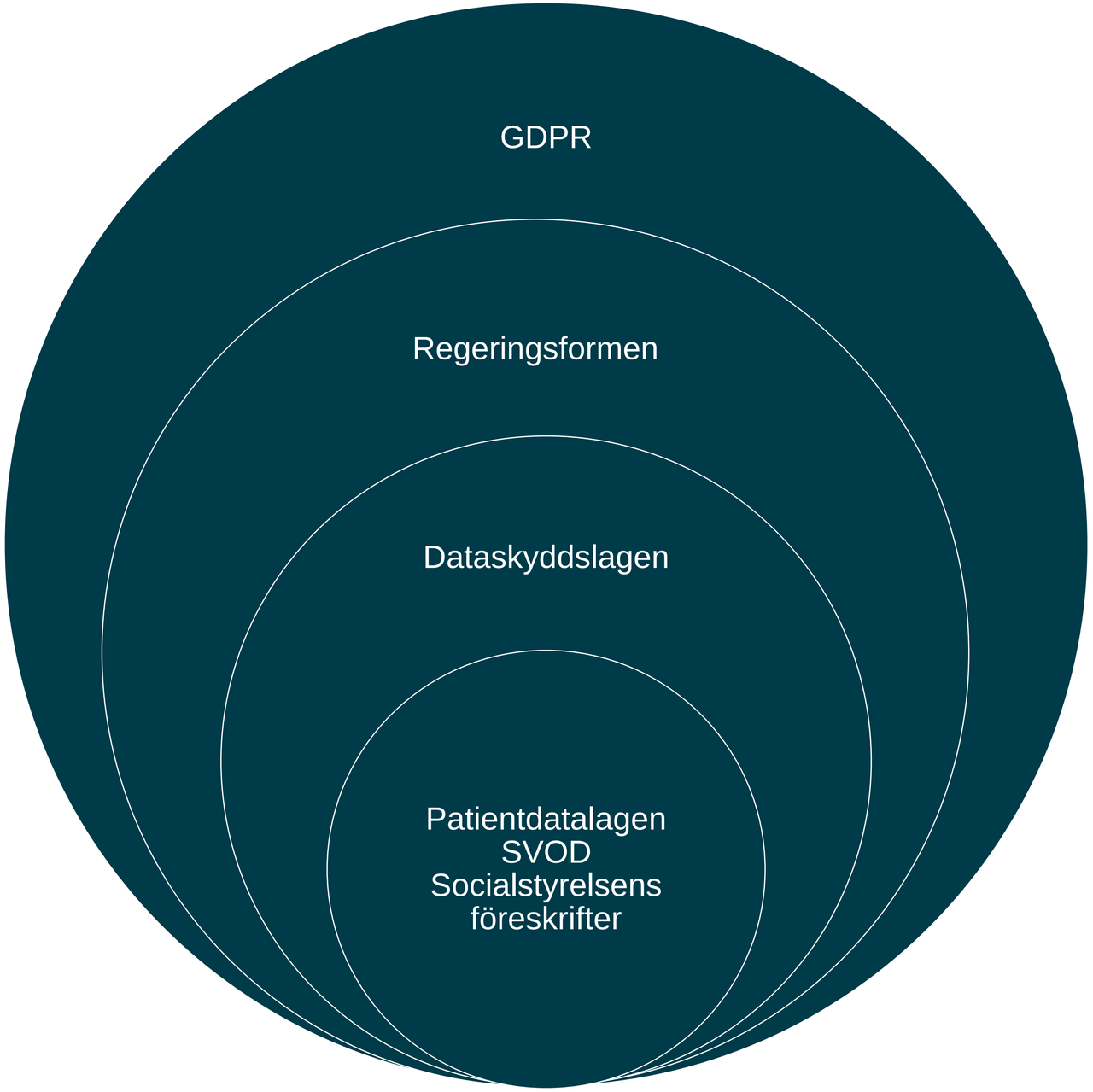
# Agenda

- Varför arbeta med dataskydd i hälso- och sjukvården?
- Relevanta regelverk och centrala begrepp
- Grundläggande principer och rättslig grund
- Roller och ansvar
- Enskildas rättigheter
- Informationssäkerhet
- Några sammanfattande medskick
- Frågor

# Varför arbeta med dataskydd i hälso- och sjukvården?

- Rätten till privatliv - en mänsklig rättighet
- Fritt flöde av personuppgifter inom EU
- Hantera risker ur ett brett perspektiv
- Förtroendefråga

# Relevant reglering



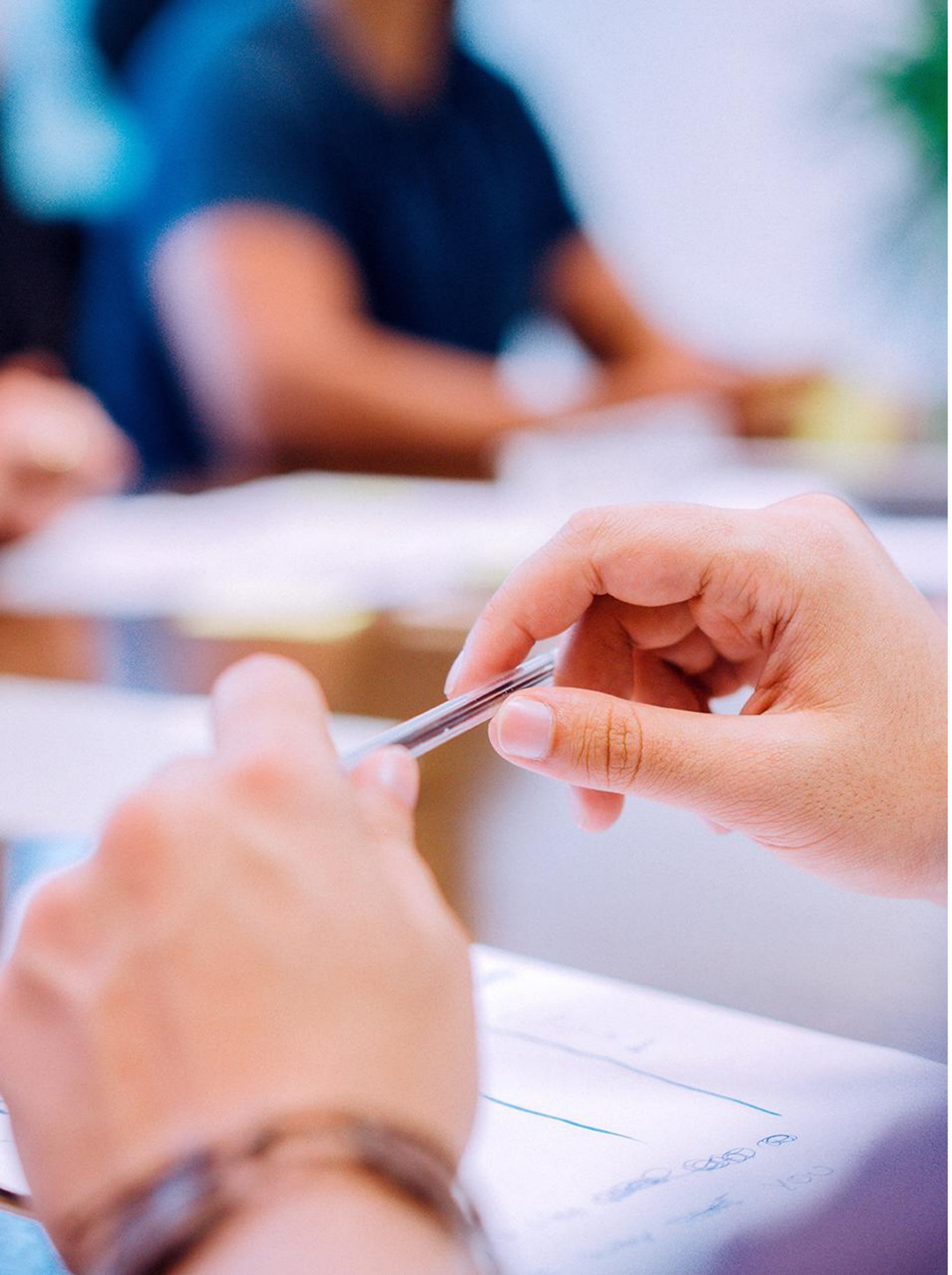

Europakonventionen och EU:s rättighetsstadga

# Centrala begrepp

- Personuppgifter
- Känsliga personuppgifter
- Uppgifter om hälsa
- Behandling
- Registrerad

# Grundläggande principer

- Principerna innebär bland annat att ni
  - måste ha stöd för behandlingen och informera om den
  - bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
    - begränsningar gäller inom hälso- och sjukvården
  - ska skydda personuppgifterna
  - ska kunna visa hur ni lever upp till GDPR



# Rättslig grund

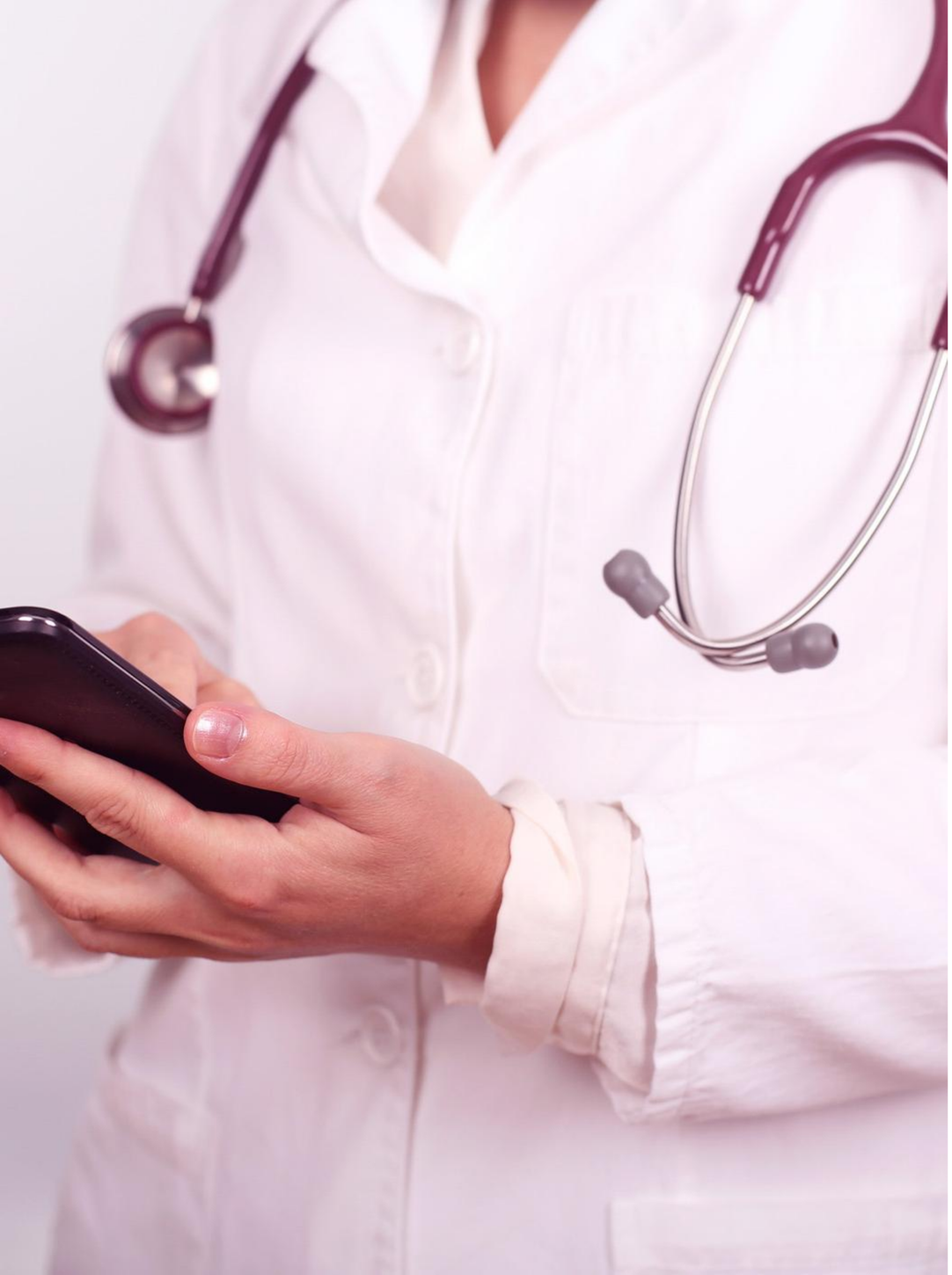
- All behandling av personuppgifter ska ha stöd i en rättslig grund.

- Exempel för vårdgivare
  - **Rättslig förpliktelse**
    - Till exempel skyldigheten att föra patientjournal
  - **Uppgift av allmänt intresse**
    - Till exempel kopplat till att ge god och säker vård

- Behandlingen ska vara nödvändig.


# Behandling av känsliga personuppgifter

- Uppgifter om exempelvis hälsa eller genetiska uppgifter
- Behandlingen är som huvudregel förbjuden.
- Undantag gäller för hälso- och sjukvården.
- Krav på tystnadsplikt enligt EU-rätt eller ett medlemslands nationella rätt



# Roller och ansvar

- **Personuppgiftsansvarig** – vårdgivaren
  - Ytterst ansvarig för behandlingen i alla led
- **Personal**
  - Behandlar uppgifter på vårdgivarens instruktioner
- **Dataskyddsombud**
  - Kontrollerar, informerar och ger råd
- **Personuppgiftsbiträde**
  - Ska följa instruktioner, men har även eget ansvar

# Enskildas rättigheter

- Rättigheter finns i flera regelverk
  - GDPR
  - Patientdatalagen
  - SVOD
  - EHDS (från 2029)

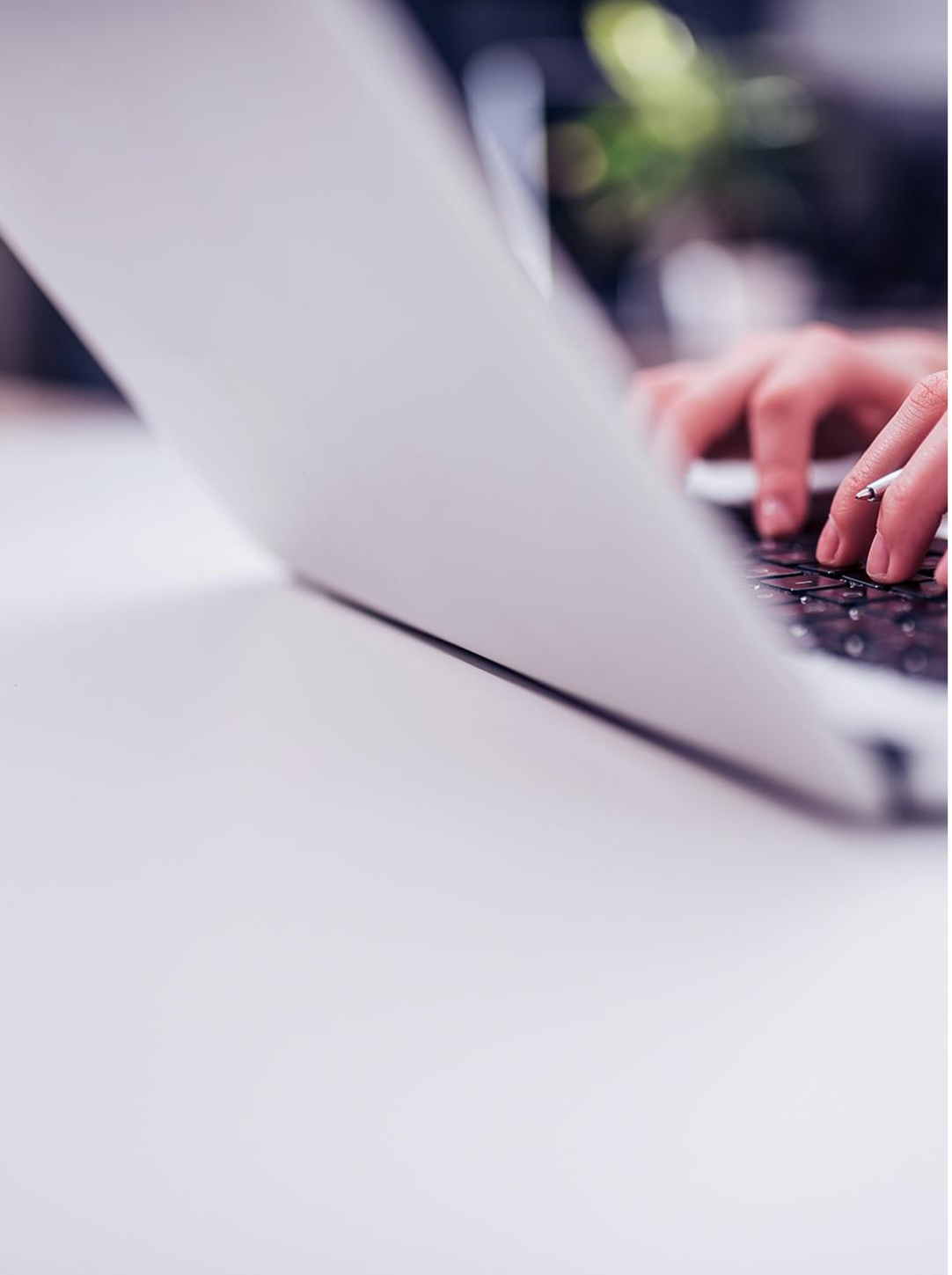
- Bland annat rätt till
  - information, till exempel om ändamål, lagringstid, mottagare, om någon har läst journalen och rättigheter
  - tillgång till de uppgifter som behandlas
  - notering i journalen

# Enskildas rättigheter, forts.

- Ni ska bland annat
  - underlätta för den registrerade
  - kunna identifiera den som gör en begäran
  - hantera en begäran så snabbt som möjligt

- Information ska ges klart och tydligt, i lätt tillgänglig form och anpassas till mottagaren.

# IT- och informationssäkerhet när personuppgifter behandlas i hälso- och sjukvården



# Varför är informationssäkerhet viktigt i hälso- och sjukvården?

- **Skyddsvärda uppgifter**: Vården hanterar några av samhällets mest känsliga personuppgifter.
- **Risker**: Dataintrång, obehörig åtkomst, felaktiga eller förlorade uppgifter kan få allvarliga konsekvenser för både patienter och verksamheten.
- **Reglering**: GDPR, patientdatalagen och Socialstyrelsens föreskrifter ställer tydliga krav på säkerhet.

# Övergripande styrning: Ledningssystem och policy

- **Ledningssystem**
  - **Tillgänglighet:** Uppgifterna ska vara åtkomliga för behöriga.
  - **Riktighet:** Uppgifterna ska vara korrekta och oförvanskade.
  - **Konfidentialitet:** Bara behöriga ska kunna ta del av uppgifterna
  - (**Spårbarhet**: Åtgärder kan spåras till en användare)
- Policy för informationssäkerhet.

# Behörighetsstyrning: Rätt åtkomst till rätt uppgifter

- Gör behovs- och riskanalys innan ni delar ut behörigheter.
- Ge behörighet efter behov: Bara den som behöver uppgifterna för sitt arbete ska ha åtkomst till dem.
- Följ upp behörigheter som har tilldelats och ändra vid behov.
- Exempel och mer vägledning på vår webb

# Kryptering: Skydda uppgifter i rörelse och vila

- Kryptering gör att obehöriga inte kan läsa uppgifterna även om de kommer över dem.

- Datas tillstånd styr typen av lämplig kryptering.
  - Data under överföring
  - Data i vila
    - Arkiverad data
    - Data under avveckling

# Exempel på tekniska åtgärder

- Flerfaktorsautentisering (MFA): Inloggning ska ske med minst två olika metoder.
- Loggning och loggуppföljning
- Systematiska och återkommande kontroller av åtkomst
- Nätverkssegmentering: Begränsa åtkomsten vid eventuellt intrång.
- Blockera USB-portar på datorer i allmänna utrymmen.
- Automatiserade larm vid misstänkta aktiviteter

# Exempel på organisatoriska åtgärder

- Fördela ansvar för informationssäkerhet genom organisationen.
- Utbilda all personal i informationssäkerhet och regelverk.
- Gör regelbundna riskanalyser och arbeta med riskhantering.
  - Identifiera risker, bestäm åtgärder och följ upp.
  - Informationssäkerhet kräver kontinuerligt arbete.
- Upprätta rutiner för att hantera säkerhetsincidenter.
- Behåll mänsklig kontroll.

# Några sammanfattande medskick

- Följ dataskyddsregleringen och annan tillämplig reglering.
- Utgå från ert uppdrag.
- Dokumentera och se konsekvensbedömning som ett stöd.
- Klargör roller och ansvar tidigt.
- Jobba med tvärfunktionellt samarbete.
- Gör det lätt för medarbetare att göra rätt.
- Bedöm och hantera risker kontinuerligt.

# Frågor?

# Lästips

- Personuppgifter inom hälso- och sjukvården
- Vägledning vid konsekvensbedömning enligt GDPR | IMY
- Vägledning om GDPR och AI | IMY
- IMY play

# Tack för att du lyssnat!
# Svara gärna på vår utvärdering

Integritetsskydds myndigheten

www.imy.se