Integritetsskydds myndigheten

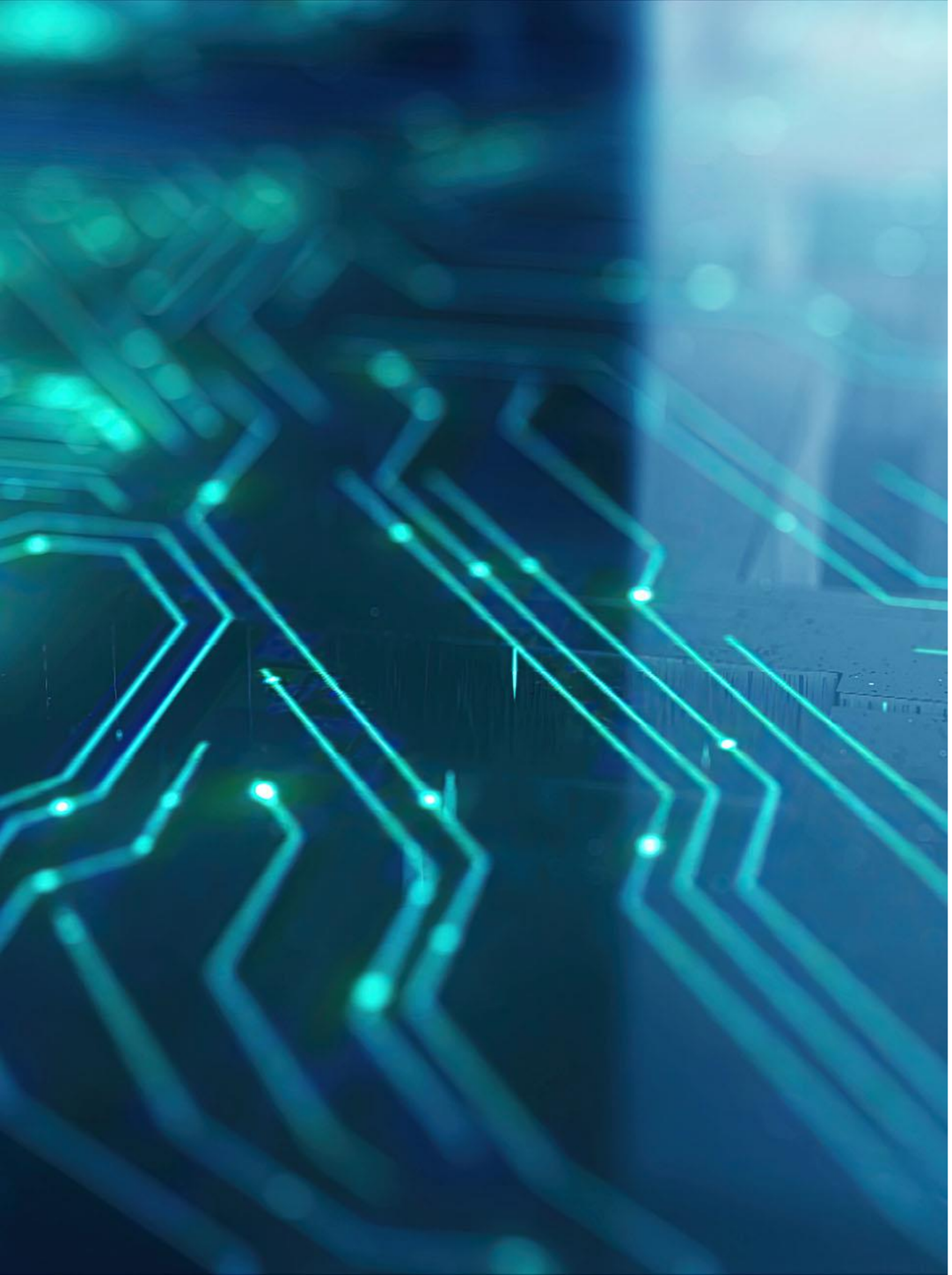
2024-10-22

Tänk säkert – agera smart

IMY deltar i

Agenda

- Säkerhet i samband med behandling
- Exempel och scenarier
  - Kryptering
  - Autentisering
  - Behörigheter
  - Säker applikationsutveckling
- Informationssäkerhetsarbete
  - Kontinuerligt och riskbaserat
- Frågestund

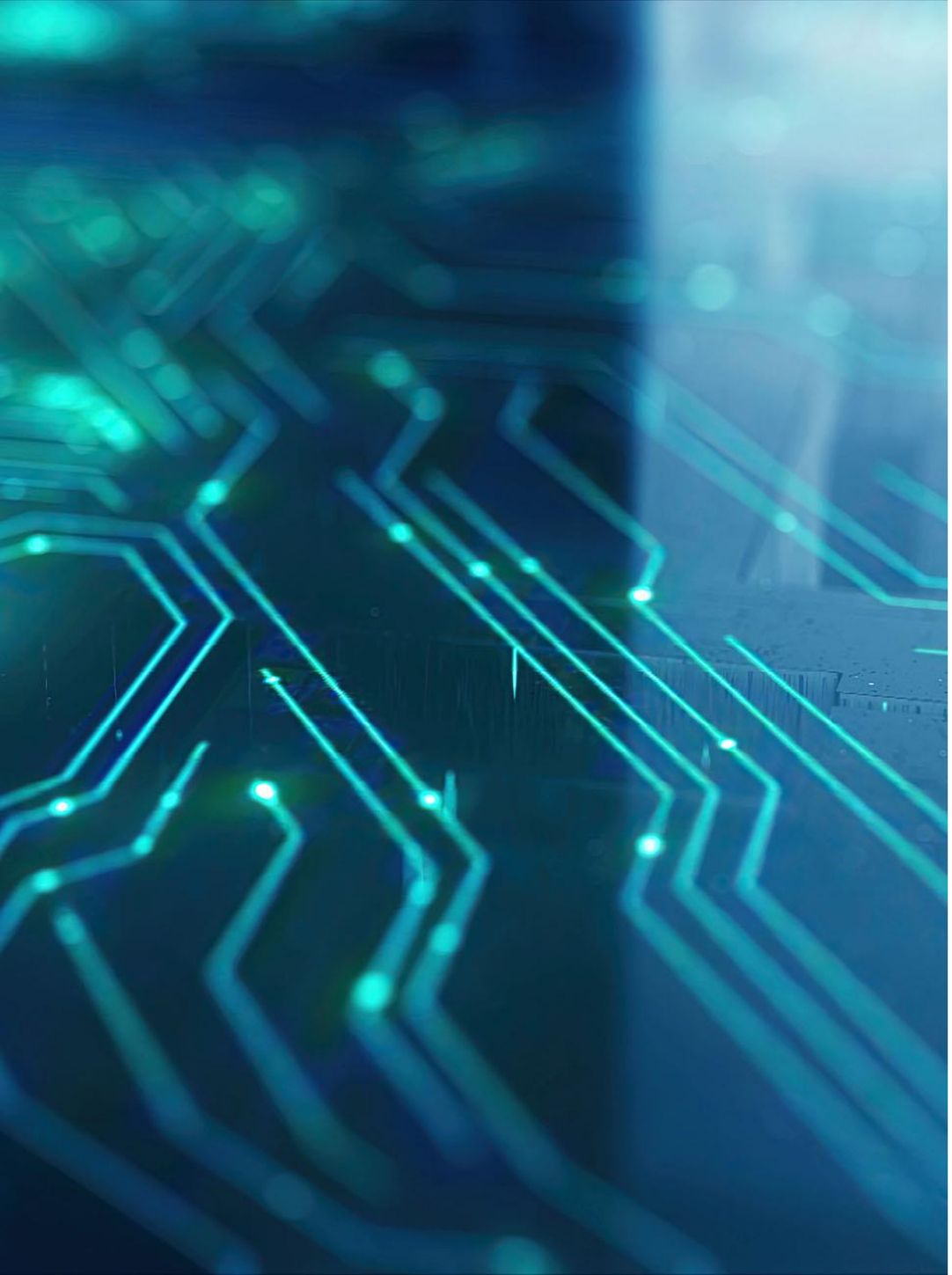


Informationssäkerhet enligt GDPR art 5.1 f

- Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna

- Inbegripet skydd mot
  - obehörig eller otillåten behandling
  - förlust, förstöring eller skada genom olyckshändelse

- Införande av tekniska eller organisatoriska åtgärder



Informationssäkerhet enligt GDPR art 32.1

Införandet av åtgärder ska göras med beaktande av

- den senaste utvecklingen
- genomförandekostnaderna
- behandlingens art, omfattning, sammanhang och ändamål
- riskerna förknippade med behandlingen

Integritetsskydds myndigheten

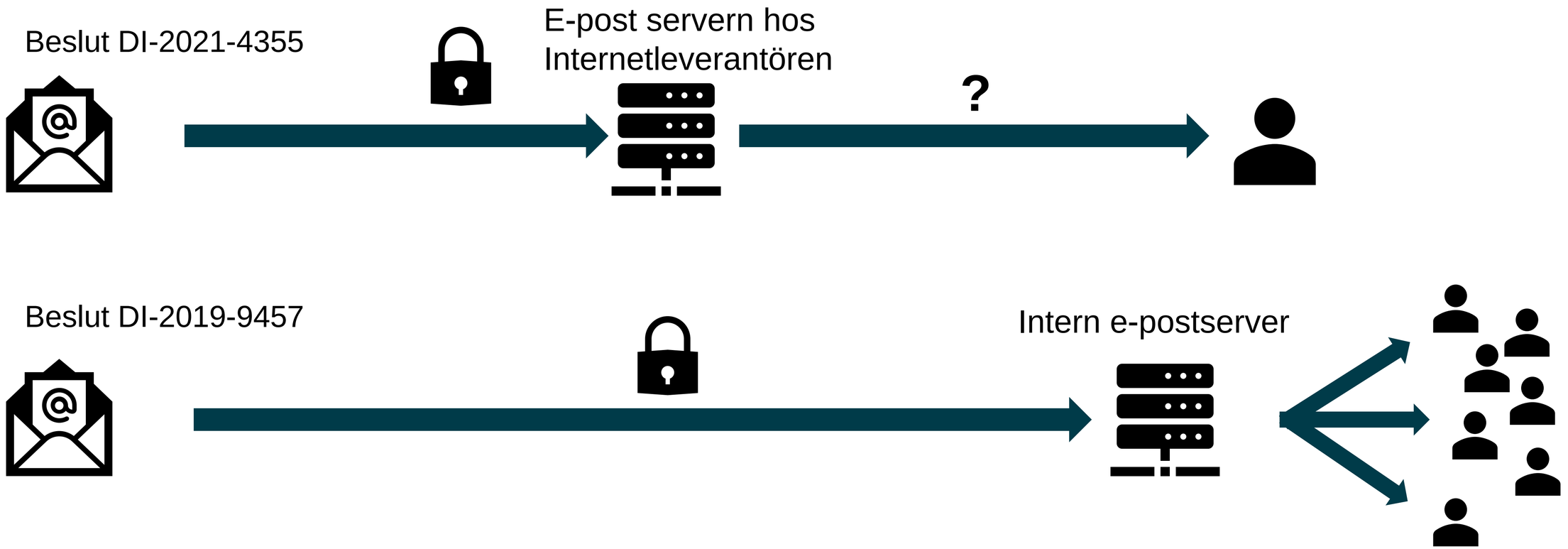
Exempel och scenarier

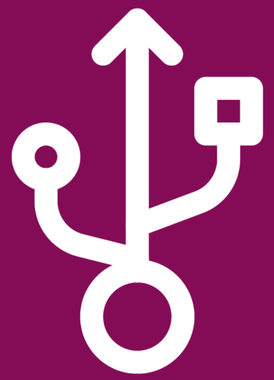
Kryptering

Varför behövs kryptering?

- Kryptering kan ofta vara en lämplig säkerhetsåtgärd
- Skyddar information vid lagring och vid överföring
- Krävs att kryptering är uppsatt på rätt sätt

Känsliga personuppgifter i e-postmeddelanden





USB-minne med känsliga personuppgifter försvinner

- På USB-minnet lagrades personuppgifter om hälsa och personnummer om 1 934 registrerade okrypterat
- Det fanns instruktioner och utbildning för vilka rutiner som gäller vid användandet av flyttbart media inkl. kryptering
- Den personuppgiftsansvarige har behandlat personuppgifter i strid med artikel 32.1
- Fungerar åtgärderna och kan man mäta effekten?

Beslut IMY-2022-1290

Några punkter att ta med sig

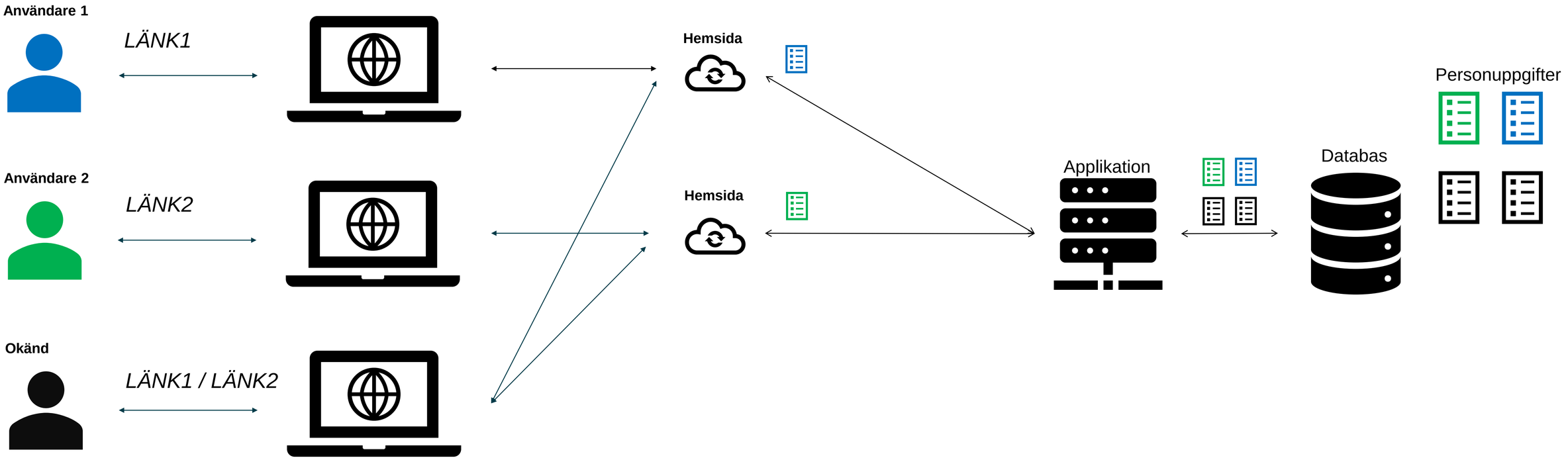
- Analysera ert behov och dokumentera
- Instruktioner till användare
- Använd tillräckligt säker kryptering
- Skydda krypteringsnycklarna
- Säkerställ att krypteringen sker hela vägen
- Krypteringen ska ske innan obehöriga kan ta del av personuppgifterna

Autentisering

Varför behövs autentisering?

- Autentisering är en åtgärd som säkerställer att en användare är den som den utger sig för att vara.
- Det behövs för en effektiv behörighetsstyrning, där endast behöriga användare kommer åt information.

Åtkomst via webb



Beslut DI-2021-1905

Några punkter att ta med sig

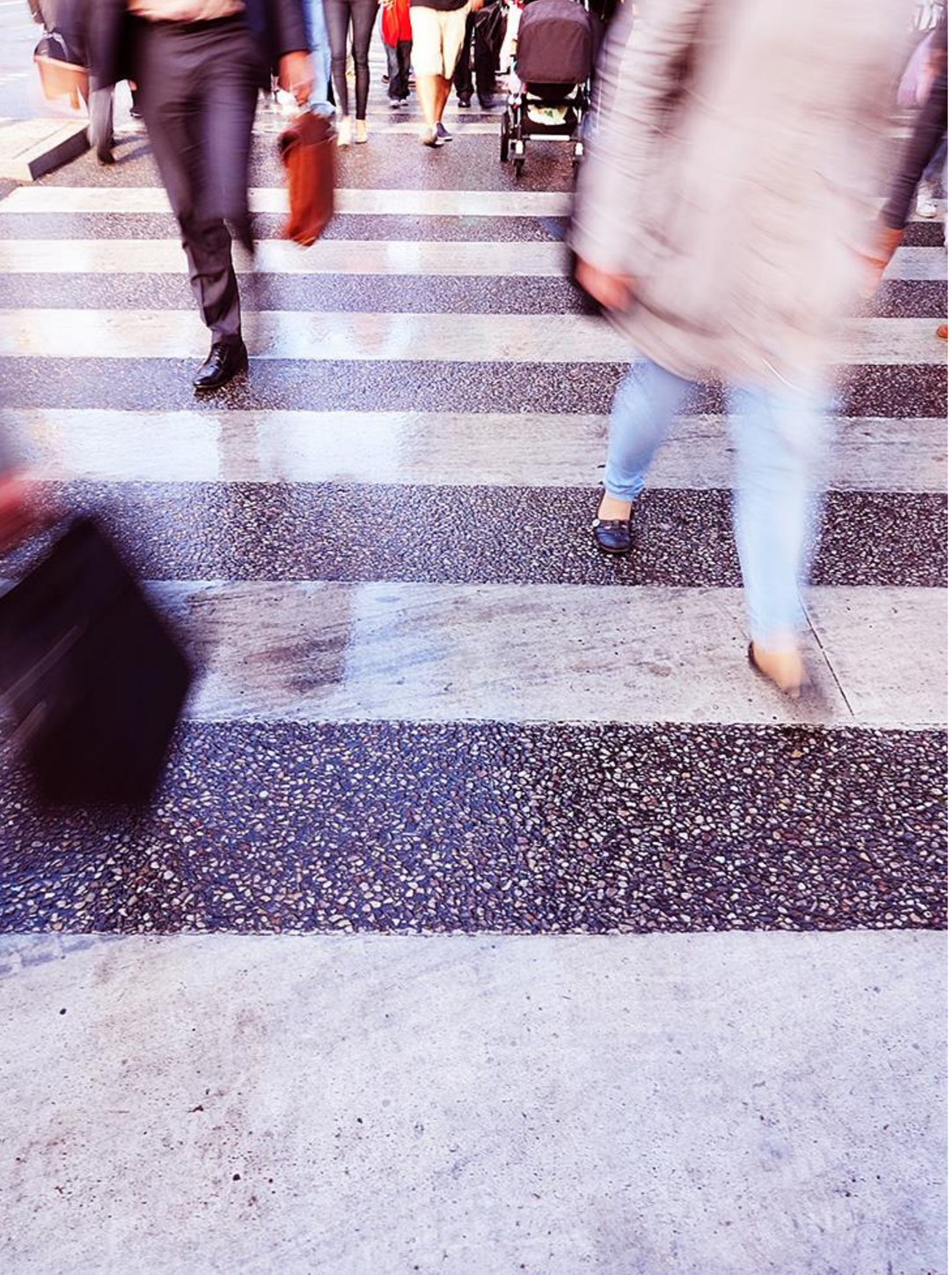
- Analysera ert behov
- Dokumentera er analys
- Instruktioner
- Logga inloggningsförsök
- Använd tillräckligt stark autentisering

Behörigheter &
Säker applikationsutveckling

(API)

Varför behövs behörighetsstyrning?

- Definierar
  - vilka uppgifter en användare har tillgång till
  - vad användaren kan göra med uppgifterna
- Grundläggande säkerhetsåtgärd för att obehöriga inte ska få tillgång till personuppgifter



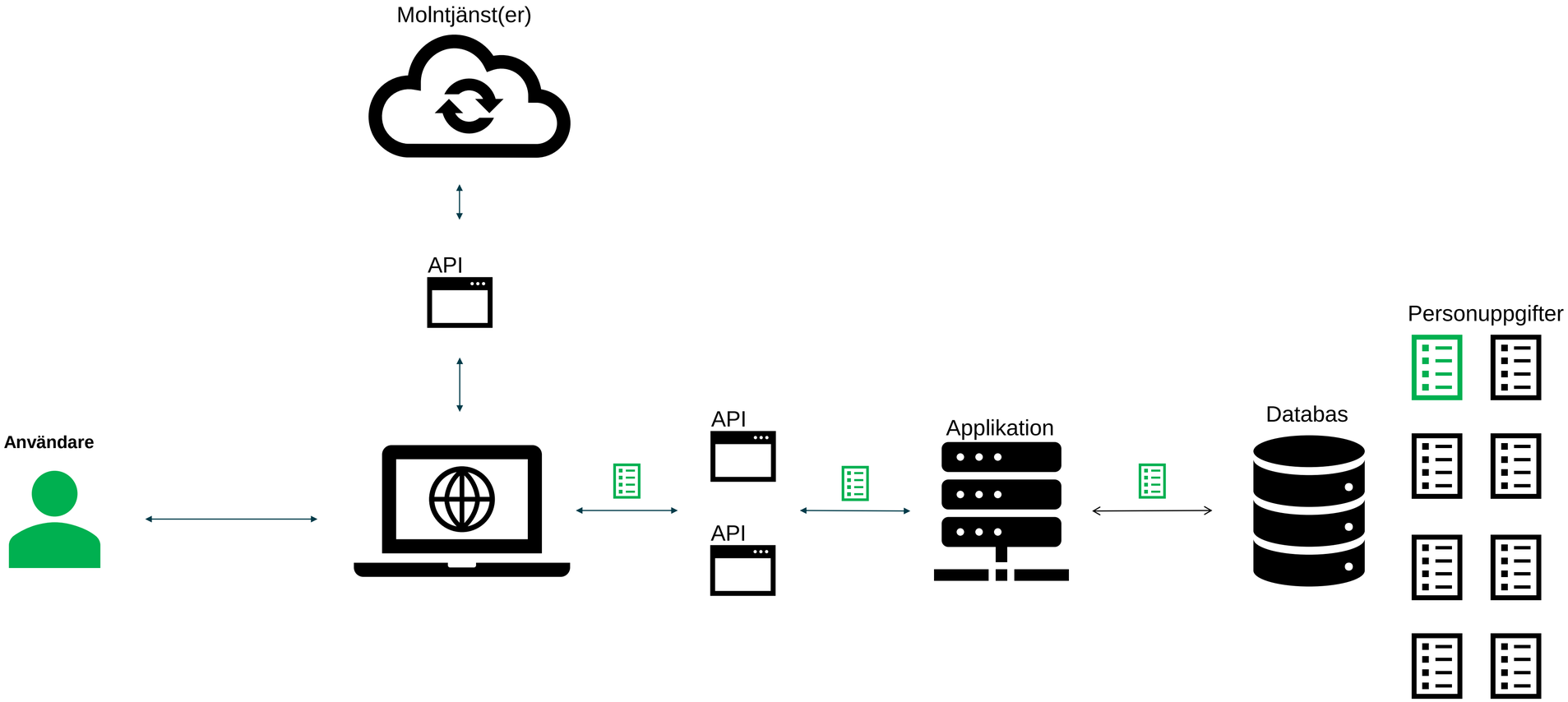
Några punkter att ta med sig

- Analysera ert behov
- Principer för åtkomst
- Använd behörighetsnivåer
- Rutiner för hantering av behörigheter
- Granska behörigheter

API säkerhet

- Vad är ett Applikationsprogrammeringsgränssnitt (API)
- Var det förekommer
- Vad är riskerna
  - Tillgång till uppgifter
  - Exponering
  - Vida behörigheter
  - Ej övervakad

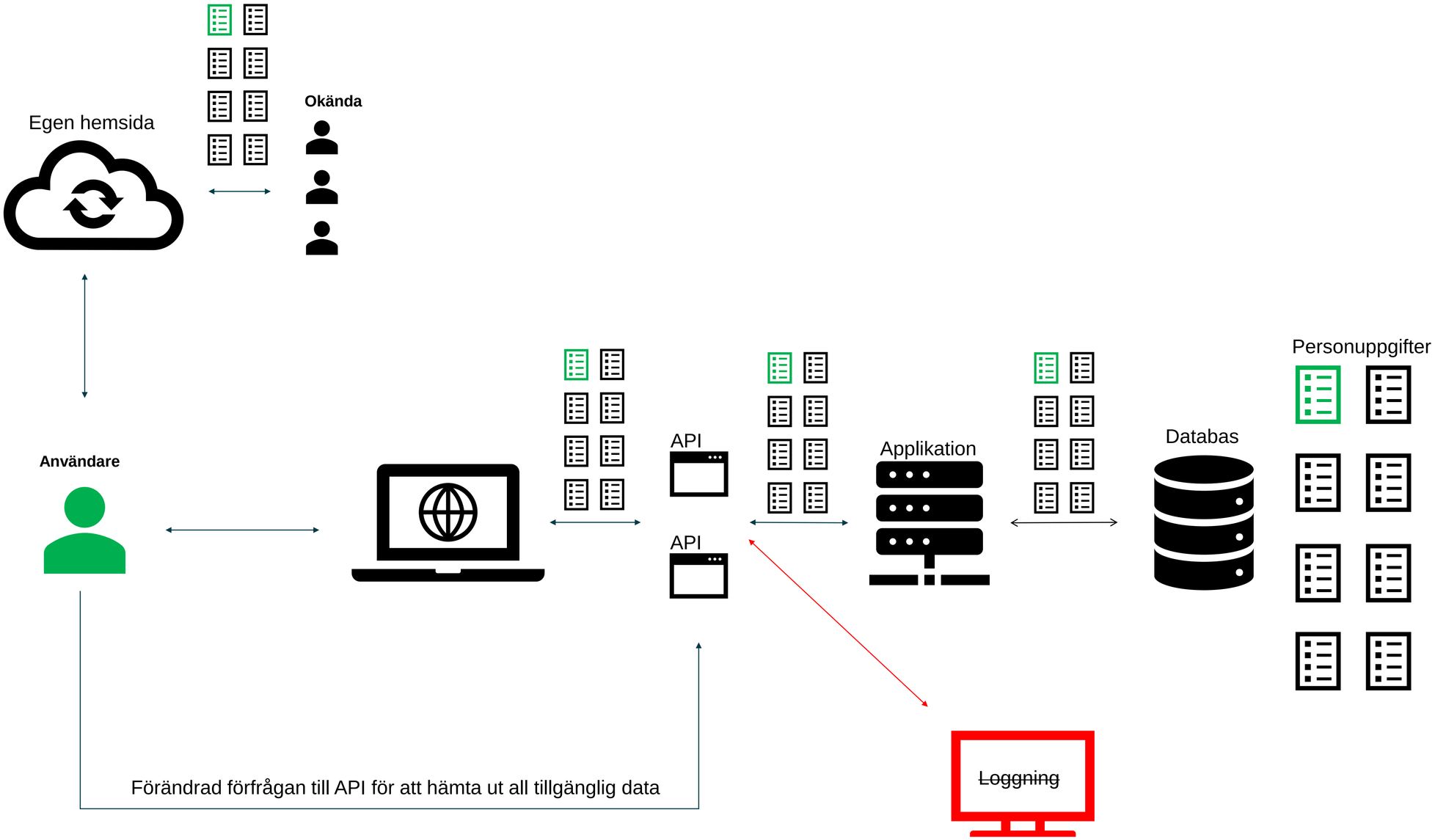
API


Molntjänst(er)
API
Användare
API
API
Applikation
Databas
Personuppgifter

Varför behövs säker applikationsutveckling?

- Ofta behandlar applikationer personuppgifter.
- Säkerställa en lämplig säkerhetsnivå i förhållande till personuppgiftsbehandlingen
- För att undvika potentiella sårbarheter.
- Det finns olika stöd för att arbeta med säker applikationsutveckling som har till syfte att öka medvetenheten kring riskerna

API



Beslut IMY-2022-9092

Några punkter att ta med sig

- Analysera designen av applikationen
- Kodgranska
- Testa säkerheten
- Dokumentera resultaten
- Säkra upp API:er

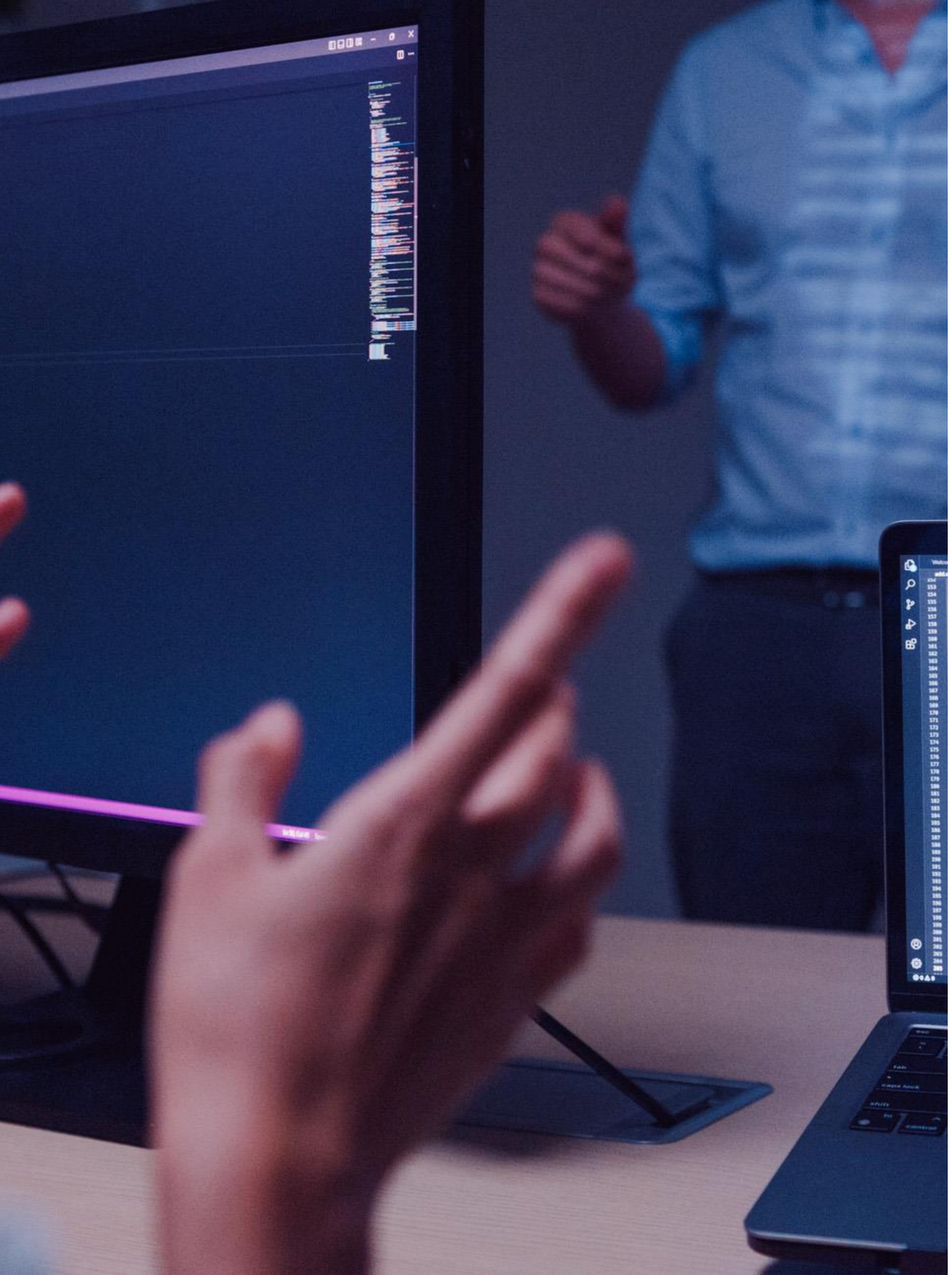
Avslutningsvis

Ett riskbaserat arbetssätt

- Beroende av de risker som personuppgiftsbehandlingen innebär för den registrerades fri- och rättigheter.
- Hög risk kräver starka säkerhetsåtgärder/hög säkerhetsnivå
- Riskbedömning ersätter inte krav på rättslig grund eller annan regelefterlevnad!
- Hög risk resulterar i krav på konsekvensbedömning och kvarstående hög risk förutsätter förhandssamråd med IMY.

Något mer om risker…

- Risker som hotar fysiska personers **grundläggande rättigheter och friheter**, särskilt deras rätt till skydd av personuppgifter.
- ”Skyddsobjekt” (vad det är som ska skyddas): behandlingen av och själva personuppgifterna.
- ”Säkerhetsmål” (syftet med skyddet eller varför de ska skyddas): upprätthållande av registrerades fri- och rättigheter.



Säkerhetsåtgärder

- Verktygen är de samma oavsett vilket perspektiv vi har
- Tekniska och organisatoriska åtgärder hänger ihop
- Följ upp och mät och utvärdera säkerhetsåtgärdernas effekt
  - Om en åtgärd inte går att mäta kan den behöva omvärderas
- Utan kontinuerlig riskanalys är det svårt att avgöra lämplig nivå på säkerhetsåtgärderna

Ett kontinuerligt riskbaserat informationssäkerhetsarbete

IMY. Integritetsskydds myndigheten

www.imy.se