IMY. Integritetsskydds myndigheten

Samordnat systematiskt informationssäkerhetsarbete - 30 min fördjupning; Säkerhet för personuppgifter

Magnus Bergström

IMY. Integritetsskydds myndigheten

Vi arbetar för att skydda alla dina personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer.

Agenda

- Ultrakort om GDPR
- Säkerhet för personuppgifter
- Artikel 32
- Lämplighetsbedömningar
- Lämpliga åtgärder - Lämplig säkerhetsnivå
- Risker

Säkerhet för personuppgifter – Informationssäkerhet enligt GDPR

- Ur skäl 39: Personuppgifter *bör* behandlas på ett sätt som säkerställer **lämplig säkerhet** och **konfidentialitet** för personuppgifterna samt förhindrar **obehörigt tillträde** till och **obehörig användning** av personuppgifter och den **utrustning** som används för behandlingen.

- Art. 5.1 f: [Personuppgifter] *ska* behandlas på ett sätt som säkerställer **lämplig säkerhet** för personuppgifterna, inbegripet skydd mot **obehörig eller otillåten behandling** och mot **förlust, förstöring eller skada** genom olyckshändelse, med användning **av lämpliga tekniska eller organisatoriska åtgärder** (integritet och konfidentialitet).

Artikel 32.1 - Säkerhet i samband med behandlingen

Med beaktande av

- den senaste utvecklingen
- genomförandekostnaderna och
- behandlingens
  - art
  - omfattning
  - sammanhang och ändamål samt
- riskerna för fysiska personers rättigheter och friheter

ska den *personuppgiftsansvarige* och *personuppgiftsbiträdet* vidta **lämpliga tekniska och organisatoriska åtgärder**…

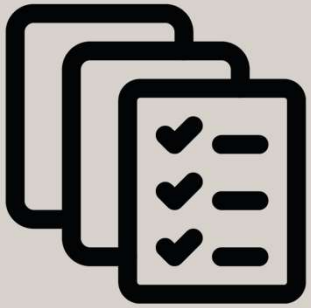
”den senaste utvecklingen” och ”genomförandekostnader”

- State of the art
  - Tillgänglig teknik
  - Standarder, såväl vedertagna och de facto
  - Myndighetsvägledningar, allmänna råd och föreskrifter
  - ”best practices” – med en liten varningsflagga här…

- Kostnad – en fråga om proportionalitet
  - Säkerhet får kosta!
  - Skydd mot orimliga krav…

”behandlingens art”

- Vilka slags uppgifter är det fråga om?
  - Integritetskänsliga uppgifter?
  - Uppgifter om en särskilt utsatt grupp?
  - Betydande maktobalans mellan PUA och den registrerade?
- Är behandlingen
  - systematisk och strukturerad?
  - tillfällig och oplanerad?
  - långvarig eller momentan?
  - förutsägbar för den registrerade?



”behandlingens omfattning”

- Antal registrerade
- Antal uppgifter om varje registrerad
- Antal personer som har åtkomst till uppgifterna
- Behandlingens geografiska omfattning

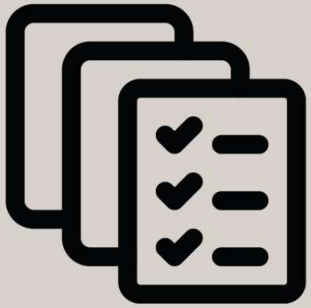
”behandlingens sammanhang”

Kan den registrerade förvänta sig en hög grad av konfidentialitet?

- Sker behandlingen i ett särskilt förtroligt sammanhang?

Man kan även se till teknisk eller organisatorisk kontext, men de övervägandena kan lika gärna hänföras till risk-resonemang…

- Hur är behandlande parter organiserade?
- Finns en eller flera personuppgiftsansvariga?
- Ett eller flera biträden?



”behandlingens ändamål”

Varför behandlar vi personuppgifterna?

Är syftet med behandlingen integritetskänslig?

- Profilering?
- Säkerhetsövervakning?
- Tillhandahålla särskilda (ev. avslöjande) tjänster?
- Kontrollera eller övervaka de registrerade?
- m.m.

Artikel 32.1 - Säkerhet i samband med behandlingen

…för att säkerställa en **säkerhetsnivå** som är lämplig i förhållande till **risken**, inbegripet, när det är *lämpligt*

a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

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.
- Högrisk resulterar i krav på konsekvensbedömning och kvarstående hög risk förutsätter förhandssamråd med IMY.
- ”Ingen hög risk, för vi vidtar så mångaoch bra åtgärder…” = feltänk!

Något mer om risker…

- Risker som hotar fysiska personers **grundläggande rättigheter och friheter**, särskilt deras rätt till skydd av personuppgifter.
- ”Security object” (vad det är som ska skyddas): behandlingen av och själva personuppgifterna.
- ”Security objective” (syftet med skyddet eller varför de ska skyddas): upprätthållande av registrerades fri- och rättigheter.
- Mer om konkreta risker finns i skäl 75 i GDPR!

Art 32.2 - Lämplig säkerhetsnivå

Vid bedömningen av **lämplig säkerhetsnivå** ska *särskild hänsyn* tas till de **risker** som behandling medför, *i synnerhet från*

- oavsiktlig eller olaglig **förstöring, förlust eller ändring** eller till
- **obehörigt röjande av** eller **obehörig åtkomst** till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Säkerhetsåtgärder

- Verktygen är de samma oavsett vilket perspektiv vi anlägger…
- Policy, anvisningar, riktlinjer, instruktioner, rutiner…
- Autentisering, behörighetskontroll, loggning, kryptering, säkerhetskopiering, nätverkssegmentering, skydd mot skadlig kod, etc…
- Kontinuitetsplanering/-hantering
- Incidenthantering
- etc

Personuppgiftsincidentanmälan

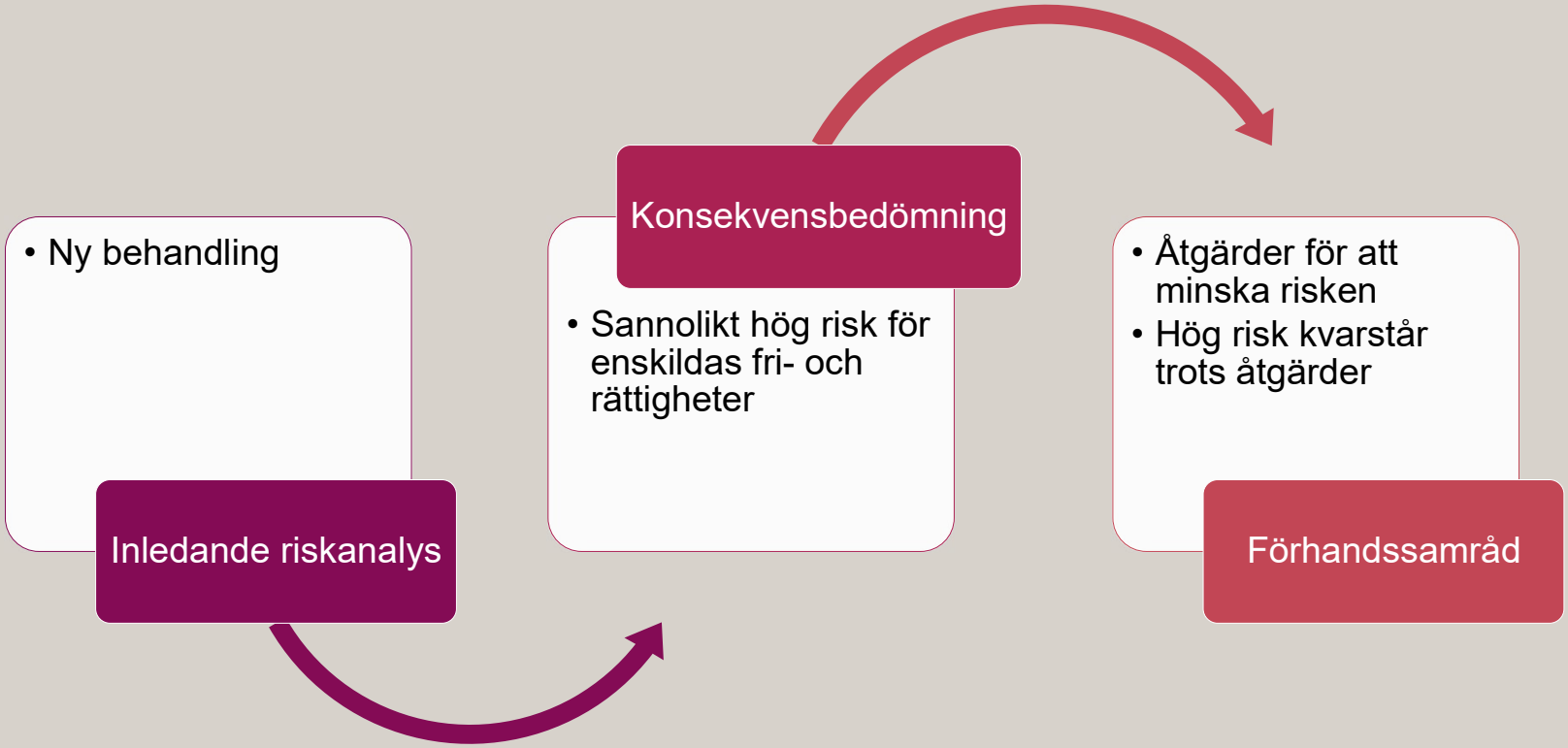
- Vad? - en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

- När? – Inom 72h - såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

- Hur? – beskriva incidentens art, sannolika konsekvenser (för fri- och rättigheter) och de åtgärder som vidtagits för att åtgärda incidenten och mildra dess effekter.

Konsekvensbedömning

Hur ser flödet ut?



Integritetsskydds myndigheten

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/

imy@imy.se

www.imy.se