

Dataskyddsförordningen (GDPR)
(och studieadministrativa system)

Syfte:

Att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till personuppgifter, och även det fria flödet av personuppgifter inom unionen.

Vem berörs?

Gäller alla som antingen är etablerade
i EU eller behandlar personuppgifter som
avser personer som befinner sig i EU

Dataskyddsdirektivet – beslutat -95 baserat på
erfarenheter från 80-talet.

Dataskyddsförordningen – beslutad -16 baserad på
erfarenheter från 00-talet

Förordningen medför en kraftig begränsning av
företags och organisationers hantering av
personuppgifter till fördel för den registrerades
rättigheter

Text från sidan 17 av 20 i ett stort och känt
företags användaravtal

”By accessing and using [företagets namn]
Services, you accept and agree to be bound by
the terms and provisions of the TOS // which
may be updated by us from time to time
without notice to you”

Konflikt

USA och EU på väg åt olika håll.

GDPR i Europa för att skydda den enskilda.

Beslut i den amerikanska senaten i våras om att ta bort lagen som hindrar ISP:er från att utföra profilering på sina kunders trafik.

Vad är en personuppgift?

”Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.”

Tidigare

”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”

Vad utgör en behandling?

”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.”

En liten parentes

PUL har undantag för personuppgifter i ostrukturerat material (så länge det inte innebär en kränkning av den registrerades rättigheter).

GDPR har det inte, men ett undantag för vad en person gör ”som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll”

Principer för all behandling enligt GDPR

- Laglig, korrekt och öppen behandling
- Korrekta och uppdaterade uppgifter
- Behandlingen skall vara säker

- Endast för uttryckligt angivna och
- berättigade ändamål
- Inte mer uppgifter än nödvändigt
- Inte under längre tid än nödvändigt

Grunder för behandling

(välj en)

- **Myndighetsutövning**
- Samtycke
- Allmänt intresse
- Tredje parts berättigade intresse
- Nödväntigt för avtal
- Rättslig förpliktelse
- Skydda den registrerades intressen

Information till den registrerade

(gäller både direkt vid insamling och vid återanvändning)

- Vilka uppgifter vi samlar in
- Vad vi ska ha dessa till
- Hur länge vi kommer att behandla dem
- Eventuell överföring
- Rätt att ta del av uppgifterna
- Rätt att klaga till Datainspektionen
- Dataskyddsombudets kontaktuppgifter

Undantag från informationsplikten vid återanvändning av personuppgifter

- Den registrerade redan är informerad
- Omöjligt eller orimligt svårt att informera
- Överföringen är föreskriven enligt lag
- Lag som föreskriver att den registrerade inte skall informeras

Register

(detta gäller för ALLA behandlingar)

- Namn och kontaktuppgifter för samtliga roller
- Ändamål med behandlingen
- Beskrivning av vad som registreras
- Vilka som har tillgång till uppgifterna
- Eventuella överföringar
- Teknisk och organisatorisk säkerhet

Den registrerades rättigheter

- Rätt till information
- Rätt att ta tillbaka samtycke
- Rätt att klaga till Datainspektionen
- Rätt att ta del av uppgifterna
- Rätt till rättelse, radering och begränsning
- Rätt att flytta sina uppgifter
- Rätt att göra invändningar och att slippa automatiserat beslutsfattande

Roller

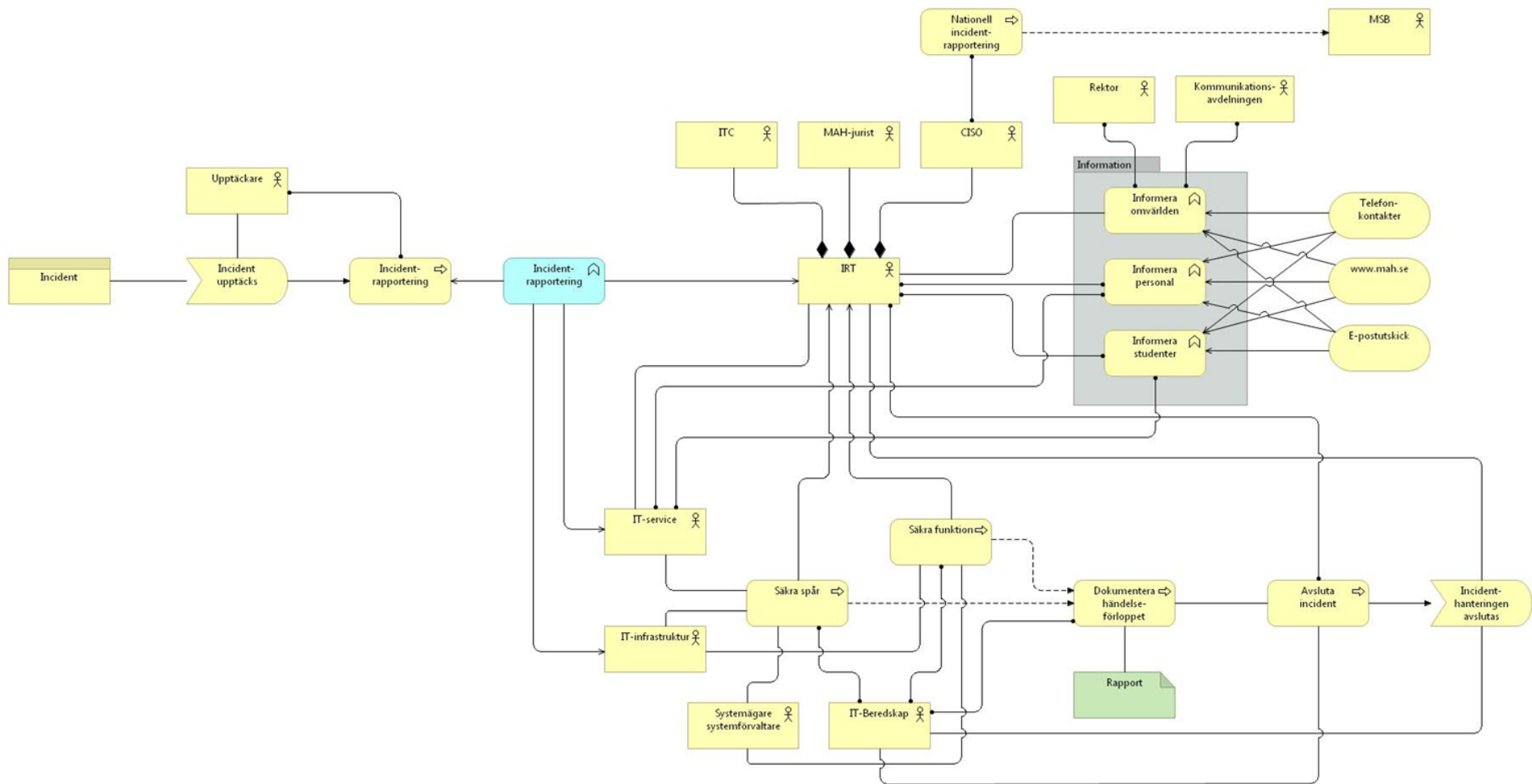
- Personuppgiftsansvarig
- Personuppgiftsbiträde
- Dataskyddsombud

Dataskydd och konsekvensbedömningar

- Lämpliga tekniska och administrativa skyddsåtgärder ska finnas på plats
- För behandlingar som sannolikt leder till en hög risk ska det göras konsekvensbedömningar
- Förhandssamråd med Datainspektionen

Incidentrapportering

- Personuppgiftsincidenter skall rapporteras till Datainspektionen inom 72h
- Information till berörda (men inte alltid)



Överföring till tredje land

- EU-kommissionen bestämmer
- EU-domstolen dömer

Undantag från förordningen

(skall fastställas i nationell lag)

- Journalistisk verksamhet
- Konstnärligt eller litterärt skapande
- Akademiskt skapande
- Tillgång till allmänna handlingar
- Arkiv av allmänt intresse, vetenskapliga, historiska eller statistiska ändamål

Sanktionsavgifter

- Skall vara effektiva, avskräckande
- och proportionerliga
- Max €20 000 000 för en svensk
- myndighet

Vad gäller mig som arbetar i ett system?

- Personuppgiftsansvarig är ansvarig
- Personuppgiftsbiträden har också ansvar
- Systemägare kommer att få anpassa och utbilda
- Medarbetare skall ta del av relevant utbildning och följa instruktioner

Anpassningar som måste göras

- Inventera och granska alla behandlingar
- Stämna av insamling mot behov
- Kontrollera rutiner för gallring
- Fastställa grunder för behandling
- Skapa informationstexter till registrerade
- Skapa utbildning för personal
- Upprätta register och incidentrapportering
- Utbilda och informera
- Semester

	Aug. 17	Sep. 17	Okt. 17	Nov. 17	Dec. 17	Jan. 18	Feb. 18	Mar. 18	Apr. 18	Maj. 18	
1	DO										
2		Möten med sys-ägare och förvaltare									
3		Möten med forskargrupper									
4	Skapa GDPR-utbildning för personal										
5		Skapa info. till reg. (A)									
6			Skapa info. till reg. (F)								
7			Skapa info. till studenter								
8			Skapa info. till handled.								
9				Webbsida							
10				Register							
11				Genomföra utbildning							
12				Registrera behandlingar							
13						Central lagring					
14						Informationsspridning					
15						Inc. rap					