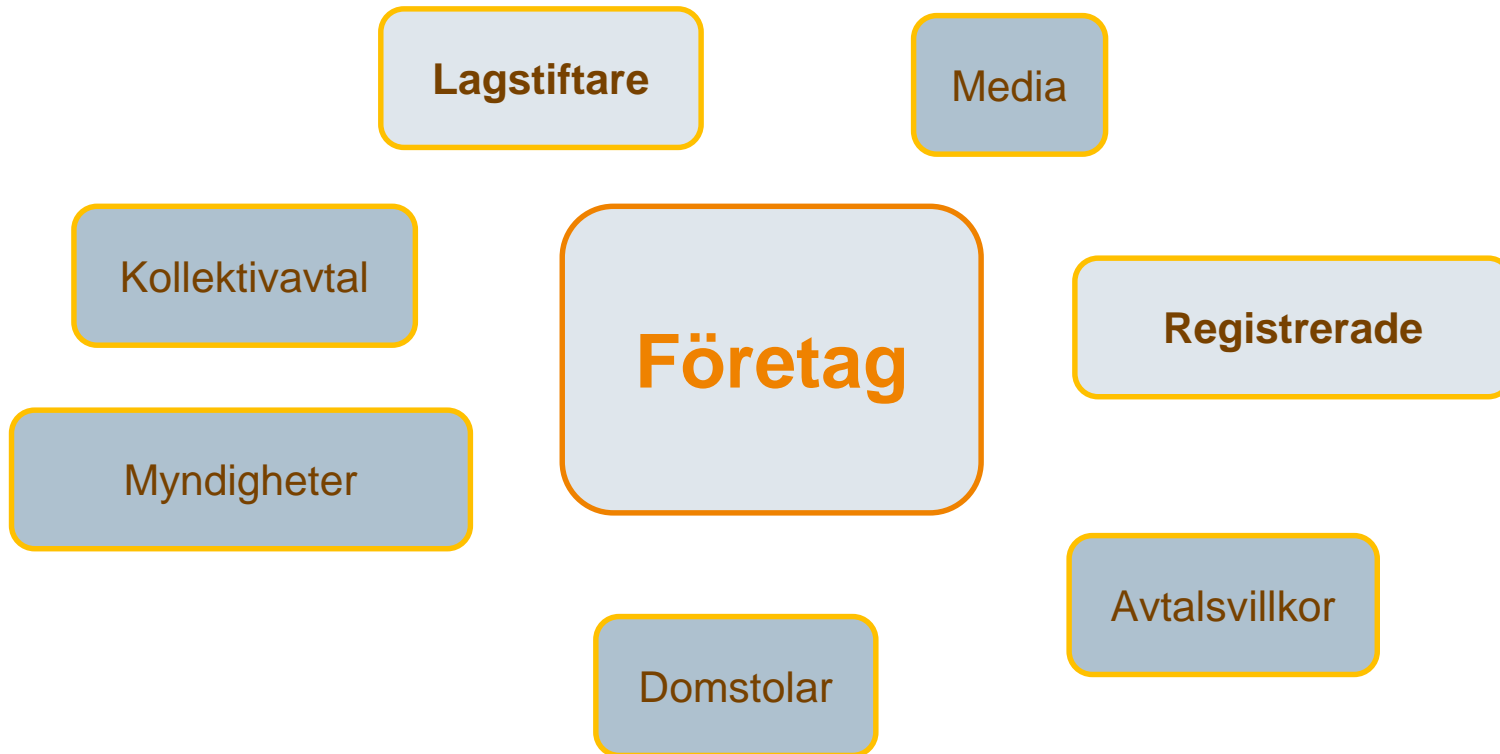


# GDPR- Vad har hänt och hur ser tillämpningen ut?



- Tillåten behandling. När kan samtycke användas?
- Rätten till information, rättning och radering
- Tillsyn

# Bakgrund: GDPR-spelarna



## Bakgrund: Dataskyddsregelverket from 25 maj 2018

---

- EU:s dataskyddsförordningen, GDPR
- Kompletterande dataskyddslag, DSL, SFS 2018:218
- Kompletterande dataskyddsförordning, SFS 2018:219
- DIFS 2018:2 , SFS
- Speciallagstiftning (*lex specialis*)

# Tillåten behandling av personuppgifter

---



# Principer

---

- Laglighet
- Korrekthet (uppdaterade, rättade, annars raderade)
- Öppenhet
- Endast för ändamålet
- Uppgiftsminimering
- Lagringsminimering
- Säkerställd integritet och konfidentialitet

## Krav på rättslig grund

---

- Samtycke (gäller ej särskilt känsliga personuppgifter)
- Fullgörande av avtal med registrerad
- Rättslig förpliktelse (lag, *kollektivavtal*, *beslut*, se *dataskyddslag 2 kap §1*)
- Skyddande av persons intressen
- Allmänt intresse eller myndighetsutövning
- Intresseavvägning (gäller ej känsliga personuppgifter)
  - Berättigat intresse PUA eller tredje part

# Samtyckets utformning

---

- Giltigt från 13-års ålder
- Klart, tydligt
- Samtycke för varje syfte
- Samtycket får inte göras tvingande
- Lika lätt att samtycka som att återkalla samtycke



# Känsliga personuppgifter

---

- Etniskt ursprung
- Politisk åskådning
- Religion
- Fackligt medlemskap
- Uppgifter om hälsa, sexualliv och **sexuell läggning**
- **Genetiska uppgifter för att identifiera en person**
- **Biometriska uppgifter för att identifiera en person**

# Tillåten behandling av känsliga personuppgifter

---

- Samtycke
- Offentliggjorda uppgifter (av den registrerade)
- Hälsa- och sjukvård (DSL kap 3, § 5)
  - Förebyggande hälsovård
  - Bedömning av arbetstagares arbetskapacitet
    - *OM villkor för tystnadsplikt uppfyllda, GDPR artikel 9.3*
- Arkiv och statistik
- Arbetsrätt, social trygghet, socialt skydd (DSL kap 3, §2)

## Arbetsrätt, DSL kap 3, § 2

---

*2 § Känsliga personuppgifter får behandlas med stöd av artikel 9.2 b i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd.*

*Personuppgifter som behandlas med stöd av första stycket får lämnas ut till tredje part endast om det inom arbetsrätten eller inom områdena social trygghet och socialt skydd finns en skyldighet för den personuppgiftsansvarige att göra det eller om den registrerade uttryckligen har samtyckt till utlämnandet.*

# Särskilt känsliga personuppgifter

---

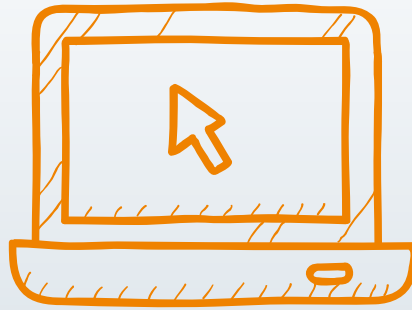
Fällande domar i brottmål samt lagöverträdelser  
” får endast utföras under kontroll av myndighet”

## Undantag

- Rättsliga anspråk (se kompletterande dataskyddsförordning)
- Tillstånd eller föreskrift från Datainspektionen (DIFS 2018:2)
- Tillåtet i annan lag eller förordning (lex specialis)
  - exempel: penningtvättslagen, visseblåsarlagen

# Information och radering

---



# Tydligare krav på att informera

---

Kontaktuppgifter för frågor

Vad informationen ska användas till

Varför företaget har rätt att behandla uppgiften

Hur länge informationen sparas

Kontaktuppgifter till Datainspektionen

## Information: registerutdrag

---

Registerutdrag ska tillhandahållas kostnadsfritt, MEN

Om begäran från en registrerad uppenbart ogrundad eller orimlig

- ta ut en rimlig avgift
- vägra att tillmötesgå begäran

# Radering av uppgifter

---

- Gallring/rensning centralt
- Rätt till rättelse
- Rätt till begränsning av behandling

- Rätt till radering och rätt att bli "bortglömd"

Privatpersoner kan begära radering "utan onödigt dröjsmål" om;

- Uppgifterna behövs inte längre
- Den registrerade återkallar sitt samtycke och annan rättslig grund saknas
- Profilerings/ direktmarknadsföring (art 21.1 och 2)
- Olaglig hantering
- Barns uppgifter (art 8.1)



## Forts radering av uppgifter

---

- Om uppgifterna är offentliggjorda informera andra PUA som behandlar
  - begränsat till rimliga åtgärder för att underrätta andra PUA om raderingsförfrågan (länkar, kopior, reproduktion)
  - beroende på tillgänglig teknik och kostnad
- Underrätta andra mottagare (inte om omöjligt eller oproportionell ansträngning)
- På begäran underrätta den registrerade om vilka som mottagit personuppgifterna

- Rätt till radering gäller inte
  - grundlagsskydd: yttrande- och informationsfrihet
  - krav i annan lagstiftning/ en uppgift av allmänt intresse eller myndighetsutövning
  - viktigt allmänt intresse på folkhälsoområdet
  - arkivändamål (allmänt intresse, forskningsändamål, statistiska ändamål)
  - uppgifter nödvändiga för att fastställa, göra gällande eller försvara rättsliga anspråk



# När görs tillsyn?

---

- Klagomål
- Media
- Bransch granskas
- Särskild typ av personuppgiftsbehandling
  - Känsliga personuppgifter
  - Nya företagsutlösningar
  - Områden med hög risk för missbruk

# Klagomål som leder till granskning

---

- Återkommande och systematiskt fel
- Allvarliga brister
- Generellt fel
- Fortsatt felbehandling

Ett klagomål är en allmän handling  
Sekretessprövning innan utlämnande

## Var kan granskning vara intressant?

---

- Dataskyddsombudspliktig verksamhet
- Personuppgiftsincidenter
- Krav på konsekvensbedömning och förhandssamråd
- Kamerabevakning
- Profilerings

# Aktuellt Datainspektionen

---

- Granskning 350 verksamheter
- 80 verksamheter saknade inrapporterad DSO
- 66 föranledde granskning
  - 2 privata vårdgivare
  - 13 fackförbund
  - 3 kollektivtrafik
  - 5 teleoperatör
  - 5 försäkringsbolag
  - 3 banker
  - 35 myndigheter
- 57 reprimander, 2 förelägganden

# Krav på konsekvensbedömning

---

- Om behandlingen hög risk för de registrerades rättigheter
- Kartlägg vilka åtgärder som behövs för riskminimering
- Personuppgiftsansvarige ska rådfråga dataskyddsombudet
- Tillsynsmyndigheten har upprättat en förteckning av det slags behandlingsverksamheter som omfattas av kravet



# Hur sker tillsyn?

---

- Inspektion: inbokad tid (i normalfallet)
- Brevväxling
- Telefon

## Vad händer? Vilken blir påföljden?

---

- Varning
- Reprimand (tillrättavisning)
- Föreläggande (beslut) att upphöra med behandlingen
- Sanktionsavgifter
  - max det högsta av
    - 200.000.000 kronor/ 4 % global koncernomsättning
  - proportionerligt

Tack! [carolina.branby@svensktnaringsliv.se](mailto:carolina.branby@svensktnaringsliv.se)

