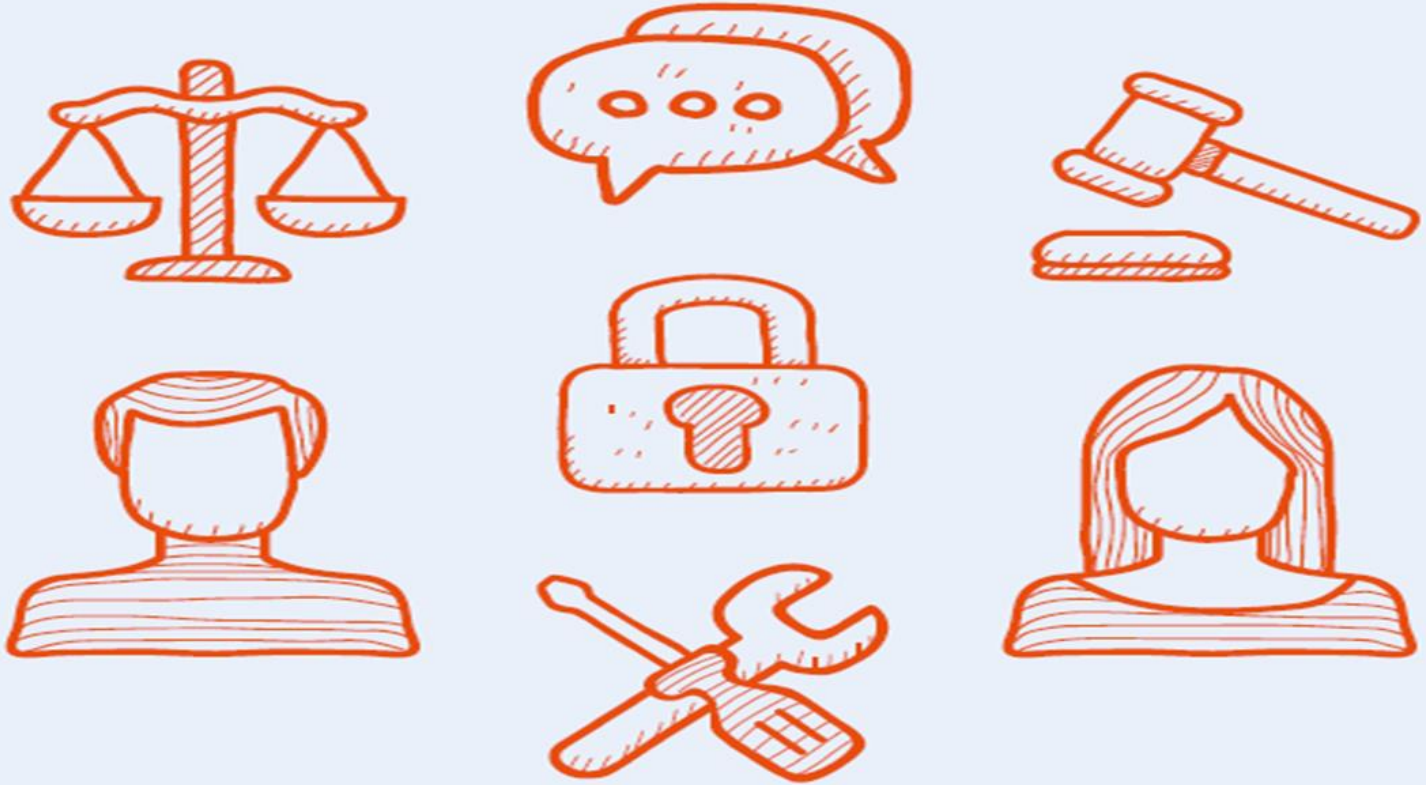
GDPR- Vad har hänt och hur ser tillämpningen ut?



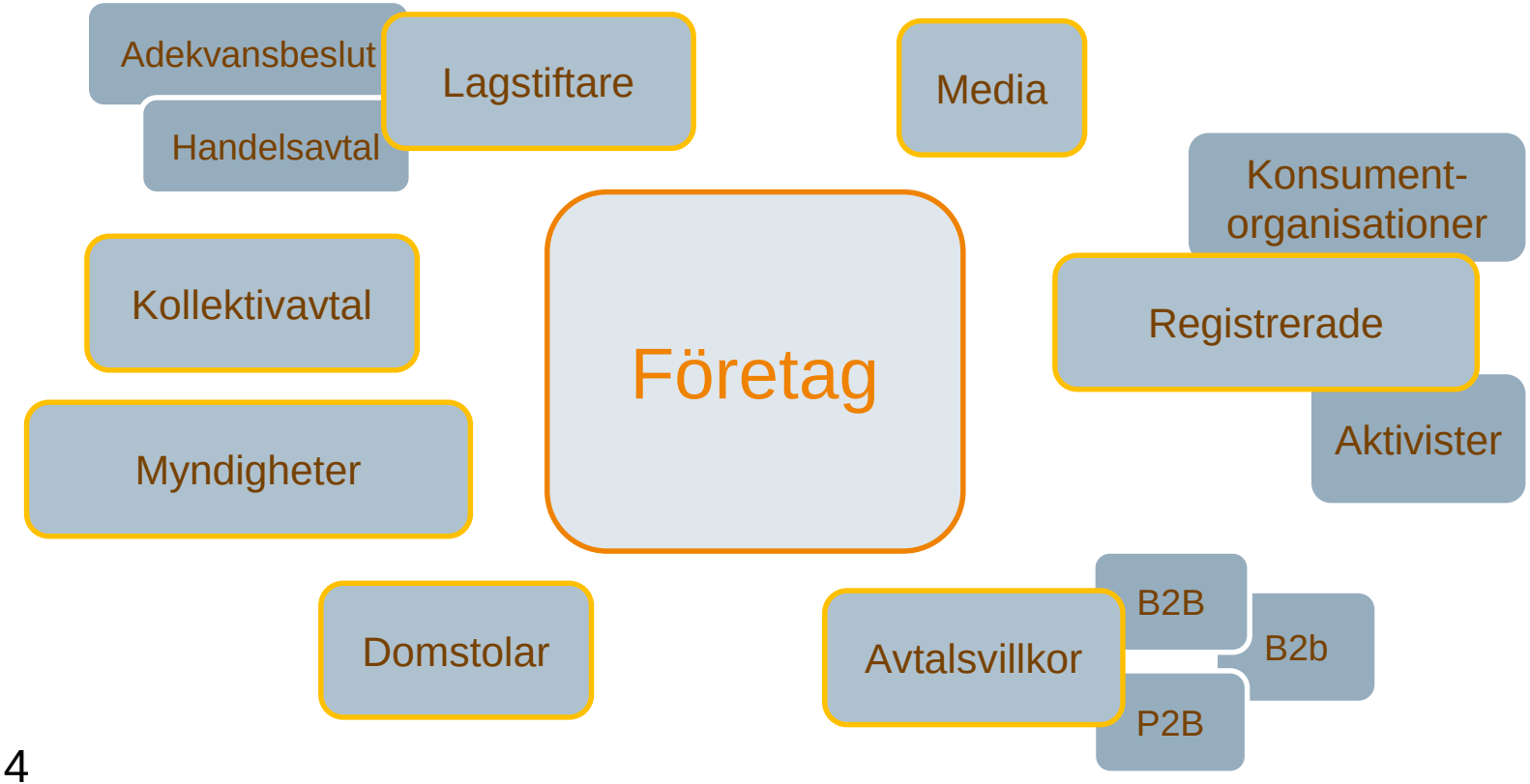
Upplägg

- Tillsyn. Dataskyddsombud, konsekvensbedömning och granskning
- Rollfördelning. Vem har ansvaret?
- Tillåten behandling. När och hur ska samtycke användas?
- Rätten till information, rättning och radering

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*)

Spelarna


Adekvansbeslut
Handelsavtal
Lagstiftare
Media
Konsument-
organisationer
Registrerade
Aktivister
Kollektivavtal
Företag
Myndigheter
Domstolar
Avtalsvillkor
B2B
B2b
P2B

Tillsyn

Krav på dataskyddsombud, DSO

- Expert
- Anmäl till datainspektionen
- Inte ha arbetsuppgifter som kan leda till intressekonflikt

Krav om kärnverksamhet

- Behandlar personuppgifter regelbundet och systematisk övervakning i stor omfattning
- Stor omfattning av känsliga personuppgifter
- Kartläggning av enskildas beteenden, sk profilering

Aktuellt Datainspektionen

- Granskning 80 verksamheter utan inrapporterad DSO
  - 66 föranledde granskning
    - 2 privata vårdgivare
    - 13 fackförbund
    - 3 kollektivtrafik
    - 5 teleoperatör
    - 5 försäkringsbolag
    - 3 banker
    - 35 myndigheter
- 1000 incidentrapporter
  - Ett utlämnande efter dom

Forts. Aktuellt Datainspektionen

- Dialogseminarium
  - It-säkerhetsbranschen
  - Detaljhandeln
  - Direktmarknadsföringsbolag
  - Arbetslivet
  - Vårdsektorn
  - Bank
  - Tele/telekombranschen

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

Forts. konsekvensbedömning

Överväg att göra en konsekvensbedömning om ni

- utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare
- behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande betydande följder för den registrerade
- systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer
- behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter.
- behandlar personuppgifter i stor omfattning
- kombinerar personuppgifter från två eller flera behandlingar på ett sätt som den registrerade inte förväntar sig, till exempel när man samkör register
- behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, exempelvis barn, anställda, asylsökande, äldre och patienter
- använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT)
- behandlar personuppgifter på ett sätt som hindrar de registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån

När görs tillsyn?

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

Var kan granskning vara intressant?

- Dataskyddsombudpliktig verksamhet
- Personuppgiftsincidenter
- Krav på konsekvensbedömning och förhandssamråd
- Kamerabevakning
- Profilering

Klagomål som leder till granskning

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

Ett klagomål är en allmän handling

Sekretessprövning innan utlämnande

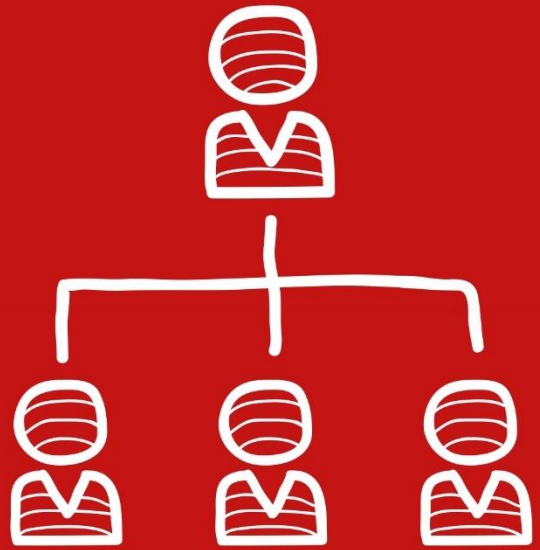
Hur sker tillsyn?

- Inspektion: normalt inbokad tid
- 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

Rollfördelning: vem har ansvaret?



Vilken roll har företaget?

- Personuppgiftsansvarig
- Självständiga personuppgiftsansvariga
- Gemensamt personuppgiftsansvarig
- Personuppgiftsbiträde

Personuppgiftsansvarig, PUA

Den juridiska personen

Personuppgiftsansvarig har kontrollansvar för personuppgiftsbiträdet

Personuppgiftbiträde, PUB

Behandlar personuppgifter åt personuppgiftsansvarig

Upprätta personuppgiftsbiträdesavtal

Personuppgiftsbiträde står delvis för ansvaret:

- Registerföring
- Tillräckliga säkerhetsåtgärder
- Anlita dataskyddsombud

Tillåten behandling av personuppgifter

Principer

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

Vad gör en behandling tillåten?

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)
- Hälso- 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 och lagöverträdelser som innefattar brott

” får endast utföras under kontroll av myndighet”

Exempel:

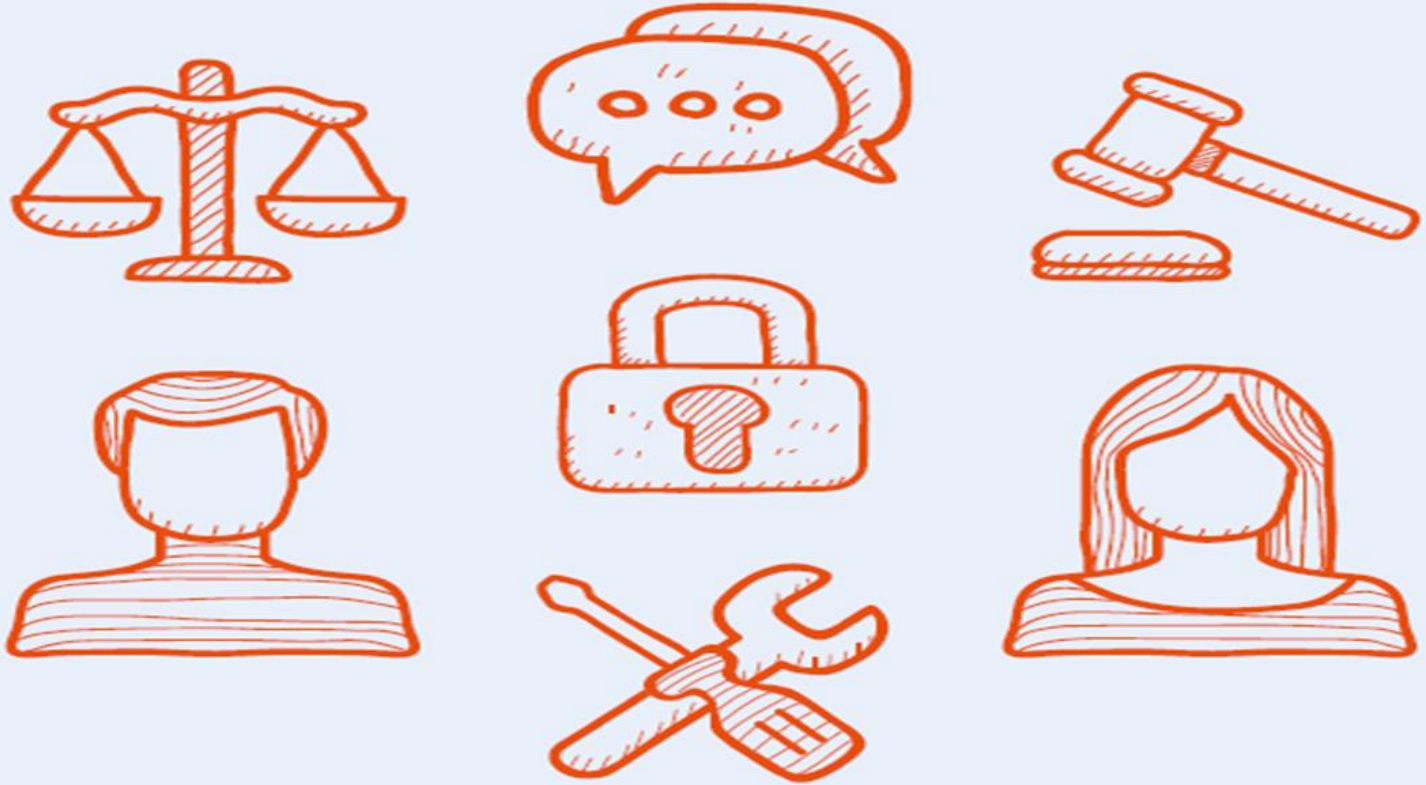
- Belastningsregisterutdrag
- *Misstanke om brott*

Undantag särskilt känsliga personuppgifter

Behandling tillåten om

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

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
  - Profilering/ 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

Forts. radering

- Rätt till radering gäller inte
  - Om behandlingen är grundlagsskyddad: yttrande- och informationsfrihet
  - Behandlingen måste ske för att uppfylla krav i annan lagstiftning/ en uppgift av allmänt intresse eller myndighetsutövning
  - Viktigt allmänt intresse på folkhälsoområdet
  - Arkivändamål (allmänt intresse, forskningsändamål, statistiska ändamål)
  - Nödvändigt att behålla personuppgifter för fastställa, göra gällande eller försvara rttsliga anspråk

Tack! carolina.branby@svensktnaringsliv.se

SVENSKT NÄRINGSLIV