# Dataskyddsförordningen

SVENSKT NÄRINGSLIV

# Dataskyddsförordningen, DSF

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävandet av direktiv 95/46/EG (allmän dataskyddsförordning)
- General Data Protection Regulation, GDPR
- 25 maj 2018
- Ersätter personuppgiftslagen, PUL

# Kompletterande dataskyddslag föreslagen

- Dataskyddsförordningen, DSF, direkt tillämplig
- Vissa artiklar förutsätter eller tillåter nationella bestämmelser
  - Preciseringar
  - Undantag

- Riksdagsbeslut i februari 2018

½

# Normkonflikt

- Grundlag företräde framför vanlig lag
- EU-rätt företräde framför svensk lag
- Speciallag företräde framför generell lag
  – ”Sektorspecifika bestämmelser ska ha företräde framför dataskyddslagen”
  MEN
  – ”…måste vara förenlig med dataskyddsförordningen och avse en fråga som får särregleras genom nationell rätt”

# Begreppet personuppgift

# Personuppgifter, exempel

- Adress
- Namn
- Personnummer
- Enskilda firmor
- Fotografier
- IP-adresser
- ”Nicks”

# 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

# Särskilt känsliga personuppgifter

Fällande domar i brottmål och lagöverträdelser som innefattar brott

” får endast utföras under kontroll av myndighet”

Exempel:

- Belastningsregisterutdrag
- Misstanke om brott

# 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)
- Skyddande av persons intressen
- Allmänt intresse eller myndighetsutövning
- Intresseavvägning (gäller ej känsliga personuppgifter)
  - Berättigat intresse PUA eller tredje part

# Tillåten behandling: känsliga personuppgifter

- Samtycke
- Arbetsrätt eller kollektivavtal
- Offentliggjorda uppgifter (av den registrerade)
- Hälso- och sjukvård (tystnadsplikt)
  - Förebyggande hälsovård
  - Bedömning av arbetstagares arbetskapacitet
- Arkiv och statistik

# Undantag särskilt känsliga personuppgifter

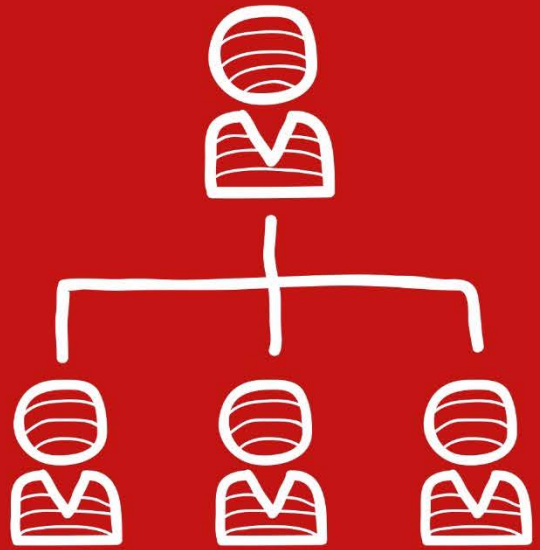
- HR: får ej behandlas!
- Ta del av/ läs, tex krav i skollagen

- Undantag
  - Enstaka uppgifter hos arbetsgivare, tex polisanmälan
  - Tillstånd från Datainspektionen
  - Tillåtet i annan lag eller förordning

# Personnummer

- Samtycke
- Intresseavvägning ”klart motiverat” av
  - ändamålet
  - säker identifiering
  - annat beaktansvärt skäl

# Ansvarsstruktur



# 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

# Dataskyddsombud

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

# Nyheterna i dataskyddsförordningen och dataskyddslagen

SVENSKT NÄRINGSLIV

# Samtyckets utformning

Högre krav

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

# 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

# Begränsning i rätten att få information

Registerutdrag ska tillhandahållas kostnadsfritt, MEN

Om begäran från en registrerad är uppenbart ogrundad eller orimliga får den personuppgiftsansvarige

- ta ut en rimlig avgift
- vägra att tillmötesgå begäran

# Begränsningar för ostrukturerat material

- Förslag att undanta registrerades rätt till utdrag
  - Personuppgifter i löpande text, tex minnesanteckningar eller PM som;
    - Inte lämnats till tredje part
    - Inte enbart statistik eller arkivändamål
    - Inte behandlats längre än ett år

# Radering av uppgifter

- Rensning fortsatt centralt
- Privatpersoner kan begära radering, ”rätten att bli bortglömd”
- Ska ske ”utan onödigt dröjsmål”

# Inbyggt dataskydd

IT-struktur viktig

Hantera krav genom system som möjliggör efterlevnad

Kryptering

# Anmälningsplikt om dataincident

- Personuppgiftsincidenter ska anmälas till tillsynsmyndigheten
- Dataintrång
- Oavsiktlig förlust av uppgifter
- Ska ske utan onödigt dröjsmål – inte senare än 72 timmar efter vetskap

# Information om dataincident

- Personuppgiftsincident ska anmälas till den registrerade OM incidenten leder till hög risk för fysiska personers rättigheter och friheter.

- OBS! Inte krav på inom 72 timmar.

- Behöver inte ske om det skulle inbegripa en oproportionell ansträngning. I så fall ska allmänheten informeras.

# Krav på dataskyddsombud

Krav om kärnverksamhet

- Behandla personuppgifter som medför regelbunden och systematisk övervakning i stor omfattning
- Stor omfattning av känsliga personuppgifter
- Kartläggning av enskildas beteenden

# Krav på konsekvensbedömning

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

# Möjlighet till dataportabilitet

- OM behandlingen bygger på samtycke och behandlingen sker automatiserat

- De registrerade ska ha rätt att få ut sina personuppgifter som lämnats till och genererats hos en personuppgiftsansvarig

- Ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig
  - Företaget ska föra över om tekniskt möjligt till annan leverantör

# Uppförandekoder

- Tillämpning av godkända uppförandekoder för att visa att den personuppgiftsansvarige fullgör sina skyldigheter

# Datainspektionens befogenheter

Tillsynsmyndigheternas befogenheter ökar

- Förhandskontroller som rör riskfylld behandling
- Kan utdöma ”administrativ sanktionsavgift”
- Enskilda ska kunna vända sig till ”sin” tillsynsmyndighet, även om klagomålet gäller ett företag i ett annat EU-land

# Sanktionerna

Den administrativa avgiften kan högst uppgå till

- 20 miljoner euro, eller
- 4 % av den globala årsomsättningen (koncernnivå)

Hur allvarlig?
Medveten eller oavsiktlig?
Åtgärder för att minska skadan?
Ekonomisk vinning?

Preskriptionstid fem år

# Export av uppgifter (utanför EU)

- Adekvatsbeslut
  - Av EU-kommissionen godkända länder, tex Privacy Shield med USA
- Godkända standardavtalsklausuler (standard contractual clauses, SCC)
- Avtal för koncern (artikel 47 DF) (binding corporate rules, BCR)
- Tillstånd av datainspektionen

# Åtgärder att vidta inför de nya reglerna

# Glöm inte

Utbilda personalen

Kartlägg insamling, lagring, överföring, användning och skyddsåtgärder

Skapa rutiner - ta fram dataskyddspolicy

Bevaka nya riktlinjer från Datainspektionen

# Åtgärder att vidta, forts.

- Bygg upp kapacitet för att lämna information mm
- Bygg upp kapacitet för att hantera intrång
- Bygg in skydd för personuppgifter i IT-systemen
  – ”privacy by design”
- Byt ut system/ kontrollera att de är anpassade
- Utse dataskyddsombud, om så krävs
- Har ni verksamhet i flera länder – gör en bedömning av vilken tillsynsmyndighet som kommer bedriva tillsynen

# Tack!

carolina.branby@svensktnaringsliv.se

SVENSKT NÄRINGSLIV