Lite historia och fakta

- 1973 trädde datalagen i kraft (världens första nationella integritetslagstiftning)
- 1998 trädde personuppgiftslagen i kraft (byggde på ett EU-***direktiv*** - 95/46/EG), övergångsbestämmelser fram till 2001
- Kommissionens förslag om en ***förordning*** kom 25 januari 2012
- Parlamentets förslag kom 21 oktober 2013
- Trialogförhandlingar (kommissionen, rådet och parlamentet) slutfördes i december 2015
- 14 april togs ett slutligt beslut om förordningen
- **Förordningen ska tillämpas i alla medlemsstater från och med den 25 maj 2018**
- Här hittar man texten till dataskyddsförordningen: (http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=SV)

Nationella bestämmelser

- ❖Bestämmelserna i förordningen bygger i många delar på att det finns nationella bestämmelser.
- **Omfattande lagstiftningsarbete kommer att krävas.**
  Det pågår nu ett lagstiftningsarbete i Sverige för att anpassa lagar till Dataskyddsförordningen. Uppdraget ska redovisas senast den 12 maj 2017
  http://www.regeringen.se/rattsdokument/kommittedirektiv/2016/02/dir.-201615/
- ❖Det förutsätts att detta arbete är klart till dess att vi ska börja tillämpa förordningen i Sverige

Några exempel på definitioner - artikel 4

- **Personuppgift** (ungefär som idag)

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

- **Behandling** – ungefär som idag
- **Begränsning av behandling**
  - ✓ markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden
- **Profilering** – nytt
- **Pseudonymisering** – nytt
- **Personuppgiftsansvarig**
- **Personuppgiftsbiträde**
- **Mottagare** – den till vilken uppgifter lämnas ut

- **Personuppgiftsincident** – nytt
  - 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.
- **Genetiska uppgifter** – nytt
  - ✓ som rör genetiska kännetecken
- **Biometriska uppgifter** – nytt
  - ✓ fysiska , fysiologiska eller beteendemässiga kännetecken t.ex. fingeravtryck och ansiktsbilder
- **Uppgifter om hälsa** – nytt
  - ✓ även uppgifter om tillhandahållande av hälsovård
- **Informationssamhällets tjänster**
  - tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare

Principer om behandling av personuppgifter – artikel 5

- Motsvarar 9 § PuL – inga större förändringar
  - ✓ a) ***laglighet, korrekthet och öppenhet***
  - ✓ b) ***ändamålsbegränsning*** (särskilda, uttryckligt angivna och berättigade ändamål, ej behandla för oförenliga ändamål)
  - ✓ c) ***uppgiftsminimering*** (adekvata, relevanta, ej för många)
  - ✓ d) ***korrekthet*** (korrekta, uppdaterade, rättas utan dröjsmål)
  - ✓ e) ***lagringsminimering*** (ej spara längre än nödvändigt)
  - ✓ f) ***integritet och konfidentialitet*** (uppgifterna ska skyddas mot obehörig eller otillåten behandling m.m.)
  - ✓ ***Ansvarsskyldighet*** (den personuppgiftsansvarige ska kunna ansvara för och kunna visa att punkterna ovan efterlevs)

Laglig behandling av personuppgifter – artikel 6

- **Motsvarar 10 § PuL**
  - a) samtycke, eller nödvändig behandling för
  - b) fullgöra avtal
  - c) rättslig förpliktelse för den personuppgiftsansvarige
  - d) skydda intressen som är av grundläggande betydelse för den registrerade (tidigare vitala intressen)
  - e) arbetsuppgift av allmänt intresse eller **led i myndighetsutövning**
  - f) intresseavvägning
- Lagstiftaren får precisera tillämpningen

Villkor för samtycke – artikel 7

- Viljeyttring som ska vara
  - ✓ frivillig
  - ✓ specifik
  - ✓ informerad
  - ✓ otvetydig
- Som ges genom
  - ✓ uttalande eller
  - ✓ entydig bekräftande handling
- Personuppgiftsansvarig har bevisbördan
- Ska vara lika lätt att återkallas som att ges

Behandling av särskilda kategorier av personuppgifter – artikel 9

- Uppgifter som avslöjar
  - ✓ ras eller etniskt ursprung,
  - ✓ politiska åsikter,
  - ✓ religiös eller filosofisk övertygelse,
  - ✓ medlemskap i fackförening
- Behandling av
  - ✓ genetiska och biometriska uppgifter
- Uppgifter om
  - ✓ hälsa, sexualliv och sexuell läggning

Behandling av särskilda kategorier av personuppgifter – artikel 9 (forts)

- Behandling av särskilda kategorier av personuppgifter är förbjuden
- Undantag

  a) uttryckligt samtycke (om inte lagstiftning säger att samtycke inte gäller)

  b) skyldigheter och rättigheter inom arbetsrätten, social trygghet och socialt skydd

  c) skydda den registrerades eller någon annans grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge samtycke

  d) stiftelse, förening, ej vinstdrivande organ (politiskt, filosofiskt, religiöst eller fackligt syfte)

  e) tydligt eget offentliggörande

Behandling av särskilda kategorier av personuppgifter – artikel 9 (forts)

- Undantag från förbudet (forts.)

  f) fastslå, göra gällande eller försvara rättsliga anspråk

  g) fullgörande av arbetsuppgift i ett viktigt allmänt intresse på grundval av lag

  h) förebyggande hälso- och sjukvård, bedömning av arbetskapacitet, diagnoser, hälso- och sjukvård, social omsorg (inklusive administration)

  i) allmänt intresse på folkhälsoområdet

  j) arkiveringsändamål för historiska, statistiska eller vetenskapliga forskningsändamål

- Flera av punkterna ovan kräver nationell lagstiftning

Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter – artikel 12

- All information ska vara begriplig och lämnas i en lätt tillgänglig form
  - ✓ ett klart och tydligt språk
  - ✓ skriftligt
  - ✓ elektroniskt
  - ✓ även muntligt (identitetskontroll krävs)
  - ✓ vid begäran om åtgärd (utdrag, rättelse, radering, begränsning, portabilitet, invändningar) ska information lämnas inom en månad

Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade – artikel 13

- När uppgifterna erhålls ska information lämnas till den registrerade om bl.a.:
  - ✓ vem som är personuppgiftsansvarig och ev. dataskyddsombud
  - ✓ syftet med och den rättsliga grunden för behandlingen
  - ✓ eventuella mottagare av uppgifterna
  - ✓ överföring till tredjeland
  - ✓ lagringsperioden och kriterier för fastställande av perioden
  - ✓ rätt till registerutdrag, rättelse, radering, begränsning, uppgiftsportabilitet och att invända mot behandlingen
  - ✓ rätt att återkalla samtycke
  - ✓ att man kan ge in klagomål till tillsynsmyndigheten
  - ✓ varifrån uppgifterna kommer
  - ✓ förekomst av profilering (bl.a. förutsedda följder)
- Behöver ej informera i den mån den registrerade redan förfogar över informationen

Den registrerades rätt till tillgång – artikel 15 (och 12)

- ”Registerutdrag” (rätt till tillgång)
  - ✓ ungefär samma regler som idag, ***dessutom*** gäller
  - ✓ möjlighet till elektroniska registerutdrag
    - ✓ art. 15.3: *”Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt om den registrerade inte begär något annat.”*
  - ✓ begriplig och lättfattlig form, även muntligt efter id-koll
  - ✓ ska lämna en kopia av de uppgifter som håller på att behandlas
  - ✓ **gratis** (för ytterligare kopior får man ta ut en administrativ avgift – om begäran är oskälig p.g.a. dess repetitiva karaktär art. 12.5)

Exempel på tuffare krav för de personuppgiftsansvariga

- Rapportering av personuppgiftsincidenter
- Registerförteckningar
- Konsekvensbedömning
- Utnämning av dataskyddsombud (tidigare lika med personuppgiftsombud men nu större ansvar)
- Sanktioner

Register över behandlingar – artikel 30

- **Personuppgiftsansvarig** och eventuella företrädare ska föra ett register över behandlingar av personuppgifter
- Följande uppgifter ska dokumenteras

  a) namn och kontaktuppgifter för personuppgiftsansvarig, ev. företrädare och ev. dataskyddsombud

  b) ändamålen med behandlingen

  c) kategorier av registrerade och kategorier av personuppgifter

  d) kategorier av mottagare

  e) ev. överföring till tredjeland

  f) tidsfrist för radering (om möjligt)

  g) tekniska och organisatoriska säkerhetsåtgärder

Utnämning av dataskyddsombudet – artikel 37

- Gäller både för personuppgiftsansvariga och personuppgiftsbiträden
- **Dataskyddsombud är obligatoriskt om**:
  - ✓ myndighet eller offentligt organ behandlar personuppgifter eller om
  - ✓ den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet kräver regelbunden och systematisk övervakning av enskilda i stor omfattning eller om
  - ✓ den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter eller personuppgifter som rör fällande domar i brottmål och överträdelser

Utnämning av dataskyddsombud – artikel 37

- Ok att utse **ett** ombud för flera företag i en koncern eller flera nämnder i en kommun el. likn. OBS! Varje nämnd/styrelse måste dock fatta beslut om att utse denne person för sin räkning.
- Anställd eller konsult – båda ok
- Ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende uppgiftsskydd

Dataskyddsombudets ställning – artikel 38

- Personuppgiftsansvarig och personuppgiftsbiträde ska
  - ✓ se till att ombudet i god tid deltar i alla frågor som rör skyddet av personuppgifter
  - ✓ stödja ombudet genom att tillhandahålla de resurser som krävs, ge tillgång till personuppgifter, underhålla hans eller hennes sakkunskap
  - ✓ se till att ombudet inte tar emot några instruktioner rörande uppdraget
- Den registrerade får kontakta ombudet
- Ombudet får inte bli föremål för påföljder för att ha utfört sina arbetsuppgifter.
- Ombudet ska rapportera direkt till högsta förvaltningsnivån

Dataskyddsombudets uppgifter – artikel 39

- Dataskyddsombudet ska ha åtminstone följande uppgifter
  - ✓ informera och ge råd till den personuppgiftsansvarige, personuppgiftsbiträdet och anställda som behandlar personuppgifter
  - ✓ övervaka efterlevnaden av förordningen, inbegripet bl.a. ansvarstilldelning och utbildning av personal som deltar i behandling av personuppgifter
  - ✓ ge råd vad gäller konsekvensbedömning
  - ✓ samarbeta med och vara kontaktpunkt för tillsynsmyndigheten

Allmänna villkor för påförande av administrativa sanktionsavgifter – artikel 83

- Böter
  - ✓ upp till 10 miljoner euro eller 2 % av globala årsomsättningen (beroende på vad som är högst) bl.a. om
    - inget dataskyddsombud
    - ingen registerförteckning
    - ingen konsekvensbedömning
  - ✓ upp till 20 miljoner euro eller 4 % av globala årsomsättningen (beroende på vad som är högst) bl.a. om
    - behandlar personuppgifter fast det inte är tillåtet
    - man behandlar särskilda kategorier av personuppgifter fast man inte får
    - inte lämnar information som krävs

Tillsynsärende från Göteborg 2012

- Konstaterar att man behandlar personuppgifter i strid med kraven i 9 § 1 st. punkterna
- **e**) de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen, och
- **f**) inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen
- förelägger därför färdtjänstnämnden att avskilja de personuppgifter som inte längre är nödvändiga för handläggningen av färdtjänsttillstånd från verksamhetssystemet
- http://www.datainspektionen.se/Documents/beslut/2012-01-16-fardtjansten.pdf

- Anders Göranson
- AnGöra AB
- Anders.goranson@angoraab.se