GDPR – General data protection regulation

Dataskyddsförordningen

TRELLEBORGS KOMMUN

Agenda

- Vad är och innebär GDPR för er organisation?
- Aktiviteter för att klara de nya kraven.
- Vad finns det för stöd?

Vad innebär GDPR?

”GDPR innebär att det blir hårdare regler kopplat till vilka personuppgifter som får behandlas och på vilket sätt personuppgifter behandlas inom en organisation.

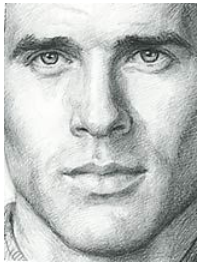
Det påverkar samtliga ställen där personuppgifter finns såsom medlemsregister, tävlingssystem, resultatlistor, licenshantering, e-post och hemsidor eller liknande”

Vad är en personuppgift?

- Information som **direkt** eller **indirekt** kan hänföras till en identifierbar fysisk person som är i livet.
- Gäller inte:
  - Avlidna personer
  - Juridiska personer
- Avidentifierade personer

Personuppgifter

- Namn
- Personnummer – Extra skyddsvärd
- Medlemsnummer
- Adress
- E-postadress
- Bilder, video & ljud
- Onlineidentifikationer & spår
  - Cookies, IP-adresser & Webbläsarhistorik



Känsliga personuppgifter

- Ras eller etnicitet
- Politiska åsikter
- Religiös övertygelse
- Facktillhörighet
- Personuppgifter om hälsa
- Sexuell läggning
- Genetiska & Biometriska personuppgifter
- Endast när det är nödvändigt exempelvis inom arbetsrätt eller myndighetsutövning

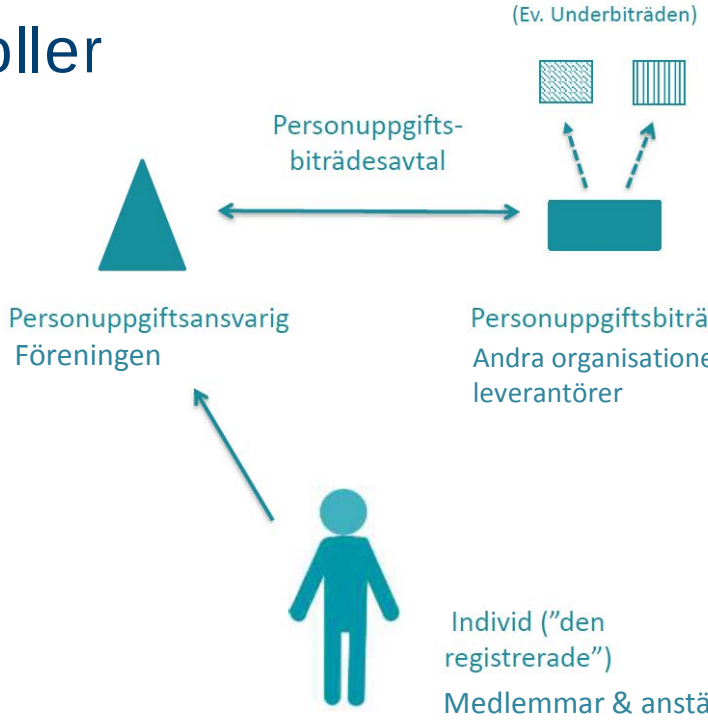
Nya dataskyddsförordningen GDPR

- Förordning för EU/EES
- Ersätter Personuppgiftslagen (PUL)
- Tillämpas från **25 maj 2018**
- Subsidär lagstiftning
- Syftar till att stärka integritetsskyddet
  - Personuppgifter en mänsklig rättighet
  - ej personuppgifter utanför EU/EES
- Missbruksregeln försvinner
  - Ostrukturerat material omfattas som mail, word och excel
- Högre sanktionsbelopp – 200 miljoner sek

För vem & vad gäller förordningen?

- Omfattar samtliga:
  - Företag
  - Myndigheter
  - Föreningar
  - Organisationer
- Undantag:
  - Privat behandling (privatpersoner)
- Gäller all behandling
  - Allt från information i system till sökbar information i en pärm
  - Undantag manuell behandling som ej är sökbar, dvs anteckningsblock, post it lappar osv.

Olika roller



Dataskyddsombud

Kontrollera
Granska
Rådgivande
Kontaktperson – Klagomål & tillsynsmyndighet

Vad innebär en behandling?

- Åtgärd/åtgärder med personuppgifter
- Arbetsprocesser
- Exempel:
  - Insamling, registrering, läsning eller radering
  - Fotografering av medlemmar, medlemsregister, administration av medlemsavgifter, resultatlistor & E-post
- Kan vara automatiserat eller manuellt

När får vi hantera personuppgifter?

- Som ett led i **myndighetsutövning**
- Arbetsuppgift av **allmänt intresse**
- Nödvändigt för att fullgöra **rättslig förpliktelse**
- Nödvändigt för att ett **avtal** med den registrerade ska fullgöras
- Skydda intressen av **grundläggande betydelse** för den registrerade eller annan fysisk person
- **Intresseavvägning**
- **Samtycke**

Intresseavvägning

Den registrerades intresse eller grundläggande rättigheter och friheter

Personuppgiftsansvariges berättigade intresse

Kan ej användas av myndigheter när de fullgör sina uppgifter

Samtycke

- Frivilligt, specifikt & tydligt
  - Kort och enkelt
- Ej beroendeställning
  - Svårt i anställningsförhållande eller myndighetsutövning
- Muntligt eller skriftligt
- Samtycke kan återkallas
- Aktivt samtycke & Separat (ej i avtal)

- Personuppgiftsansvarig som har bevisbördan

De grundläggande principerna

- Laglig, rättvis och öppen
  - Information om behandling
    - Vid inhämtande av information
      - Direkt från registrerad
      - Annat håll
    - Registerutdrag
- Ändamålsbegränsning
- Korrekthet
  - Uppdaterade

De grundläggande principerna

- Uppgiftsminimering
- Lagringsminimering
  - Lagkrav eller när ändamålet är uppfyllt
    - Dokumenthanteringsplanen
    - Arkivering, forskning eller statistik
  - Gallring
- Integritet och konfidentialitet
  - Lämplig säkerhet
  - Tekniskt och organisatoriskt
    - Utifrån vanliga personuppgifter, extra skyddsvärd information & känsliga personuppgifter
    - Exempelvis stark autentisering, kryptering osv
- Ansvarsskyldighet
  - Föreningen - styrelsen

Rättigheter och skyldigheter

- Information, tillgång, rättelse, radering, begränsningar & invändningar.
- Registerförteckning
- Personuppgiftsincident
- Konsekvensbedömning
- Barns uppgifter
  - extra
  - Åldersgräns 13
- Kontrollera efterlevnad – Rutiner & tekniska lösningar

Sanktioner

- Datainspektionen/Integritetsmyndigheten som är tillsynsmyndighet
- Administrativa sanktionsavgifter:
  - Nivå 1: 100 miljoner SEK alternativt 2 % av omsättningen
  - Nivå 2: 200 miljoner SEK alternativt 4 % av omsättningen
- Registrerad kan kräva skadestånd

Omvärldsbevakning

- Google – ska slutat skanna mejl för personlig reklam (1,2 miljarder anv)
- Svenska kyrkan
  - register om barn som inte tillhör kyrkan, men som har en eller två vårdnadshavare som tillhör kyrkan.
  - Orsaken är att kyrkan bland annat ska kunna erbjuda att låta döpa barnet eller för att bjuda in barnet till konfirmation eller någon verksamhet i församlingen (marknadsföring).
  - Att spara uppgifter i 18 är längre än nödvändigt (Uppgiftsminimering) (Lagligt men skulle raderats efter respektive marknadsföringsåtgärd var avslutad)

Vad ska ni göra nu?

- Ordning och reda!
  - Samla bara in det ni behöver
  - Gallra
  - Var lagrar vi informationen?
  - Ha koll på vem som har tillgång till informationen?
  - Rätt skydd
  - Dokumentera
- Skapa medvetenhet
- Planera för implementering
- Börja kartlägga var ni hanterar personuppgifte

Vad finns det för stöd?

- Svensk idrott håller på med ett arbete
  - Uppförandekod för idrotten
    - Vad ska samlas in för personuppgifter ?
    - Hur länge ska de sparas?
  - Genomgång av deras system
  - Mallar & Riktlinjer
  - Registerförteckning, personuppgiftsincident, registerutdrag & policys
  - Ostrukturerat material
  - Publiceras i början av mars

Kontaktuppgifter:

- Jakob.dahlman@trelleborg.se

TRELLEBORGS
KOMMUN