Dataskyddsförordningen – GDPR

Samfällighetsföreningar

Madeleine Arvidsson Wäli

Villaägarna
VILLAÄGARNAS RIKSFÖRBUND

Dataskyddsförordningen

- 1995, Dataskyddsdirektivet, resulterade i Sverige i Personuppgiftslagen, PuL
- 25 maj 2018, Allmän dataskyddsförordning
- GDPR, General Data Protection Regulation
- Gäller som lag i alla EUs länder
- Syftet var
  - Modernisering
  - Harmonisering
  - Stärkta rättigheter och klargörande av ansvar

Förändringar

- Stärkta rättigheter för den registrerade
- Samtyckesreglerna
- Missbrukregeln försvinner
- Portabilitet
- Profilering
- Administrativa avgifter, sanktionsavgifter
- Anmälansmöjligheten
- Personuppgiftsincident

Personuppgiftsansvarig

- Vanligtvis en juridisk person
- Troligen alla enskilda juridiska personer
- Varje förening är personuppgiftsansvarig
- Bestämmer ändamål och medel för behandlingen

Personuppgiftsansvarig

- Måste kunna visa att förordningen följs genom dokumentation
  - Tydliga ändamål
  - Laglig grund för behandling
  - Dokumentera behandlingar
  - Upprätta rutiner
  - Utbilda sin personal
  - Följa upp att rutiner följs

Personuppgiftsbiträde

- Alla som på uppdrag av en personuppgifts-ansvarig hanterar personuppgifter
- Partners och konsulter
- Kan vara juridisk person eller fysisk person
- Biträden har ett större ansvar än tidigare

Dataskyddsombud

- Obligatoriskt i vissa organisationer, frivilligt i andra
- Kontaktperson för registrerade
- Kontaktperson för Datainspektionen
- Rådgivande och kontrollerande roll inom organisationen
- Tystnadsplikt

- Dataskyddsambassadör

Personuppgift

- Varje uppgift som avser en identifierad eller identifierbar fysisk nu levande person
- Direkt eller indirekt identifiering
- Ska behandlas på ett sätt som uppfyller ett antal principer

Personuppgift, exempel

- Namn
- Adress
- Telefonnummer
- Personnummer
- E-postadress
- Bilars registreringsnummer
- Fotografier, filmer och ljudupptagningar
- Cookies och IP-adresser

Personuppgift, exempel

- Namnlistor på event, anmälningslistor
- Tävlingsbidrag
- Protokoll från möten, om personuppgifter anges
- Foton från event
- Medlemsmatrikel på årsmöte
- Lista med registreringsnummer på bilar
- Debiteringslängd

Känsliga personuppgifter

Kallas genom den nya förordningen ’Särskilda’

- Religiös och filosofisk övertygelse
- Politisk åsikt och fackföreningsmedlemskap
- Ras eller etniskt ursprung
- Sexuell läggning eller sexualliv
- **Hälsotillstånd**
- Biometri, film och foto (som visar t ex längd, vikt)
- Genetik

Personuppgiftsbehandling

- Alla former av lagring och hantering av data
- Gäller strukturerad och ostrukturerad material
- Gäller oavsett lagringsform, såväl papperslistor som data i digital form

Personuppgiftsbehandling

- Den enskilde äger själv alla sina personuppgifter
- All hantering ska motiveras och redovisas på ett sätt som tydligt visar
  - Vilka som finns
  - Var de finns
  - Varifrån de kommer
  - Vad de ska användas till
  - Att de är korrekta och aktuella

Principer för behandling

- Laglighet, korrekthet och öppenhet
  - Korrekthet i hanteringen
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
  - Korrekta uppgifter
- Lagringsminimering
  - Se över gallringsrutiner
- Integritet och konfidentialitet
- Ansvarsskyldighet

Principerna i praktiken

- Bestäm ändamål och håll fast vid det
  - Samla endast in uppgifter som behövs för ändamålet
  - Samla inte in fler uppgifter än nödvändigt
  - Använd inte för annat oförenligt ändamål
  - Radera uppgifter som inte längre behövs
- Identifiera rättslig grund för behandling
- Informera öppet och ärligt
- Se till att alla uppgifter är korrekta och uppdaterade

Principerna i praktiken

- Skydda insamlade uppgifter
- Se till att kunna visa att allt sker på rätt sätt
  - Dokumentera
  - Förteckning för behandlingarna
  - Rutiner och organisation
  - Dataskyddsombud
  - Uppförandekod

Personuppgiftsincident

- Oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgift
- Obehörigt röjande av personuppgift
- Obehörig åtkomst till personuppgift
- Gäller för personuppgift som överförs, lagras eller behandlas
- Ska anmälas till Datainspektionen inom 72 h

Registerförteckning

- Alla som hanterar personuppgifter ska föra register över vilka behandlingar som sker

- Varje förening måste upprätta register
- Mall för detta kan tillhandahållas

EUs rättighetsstadga

- Artikel 8 – skydd av personuppgifter
  - Var och en har rätt till skydd av de **personuppgifter** som rör honom eller henne
  - Dessa uppgifter ska behandlas lagenligt för bestämda **ändamål** och på grundval av den berörda personens **samtycke** eller någon annan legitim och **lagenlig grund**. Var och en har rätt att få **tillgång** till insamlade uppgifter som rör honom eller henne och att få **rättelse** av dem.
  - En oberoende **myndighet** ska kontrollera att dessa regler efterlevs

Rättslig grund för registrering

- **Behandlingen är nödvändig för**
  - **Avtal**
  - **Rättslig förpliktelse**
  - Grundläggande intressen
  - Uppgift av allmänt intresse
  - Myndighetsutövning
  - **Intresseavvägning**
- **Samtycke**
- **Missbruksregeln försvinner**

Avtal

- Medlemskapet är en form av avtal
- Grund för utskick av avgift
- Grund för utskick av erbjudanden
- Av ändamålen framgår vad som ingår i medlemskapet
  - Om man säljer böcker finns en liten möjlighet att spara uppgifter om en person
  - Om man istället säljer en komplett läsupplevelse ökar man möjligheten att spara uppgifter

Samtycke

- Frivilligt
- Specifikt
- Informerat
- Otvetydig viljeyttring, tydligt
- Aktivt

- Använd helst inte samtycke
  - Går att återkalla
  - Kräver stora informationsinsatser

Samtycke

- Personuppgiftsansvarig måste kunna visa att samtycke finns
- Samtycke får inte vara ett villkor
- Ska vara lika lätt att återkalla som att ge
- Nytt samtycke om ändrade ändamål
- Nytt samtycke om biträde byts ut
- Rutin för löpande översyn av lämnade samtycken måste finnas

Samtycke

- Samtyckesruta får inte vara förifylld
- Tydlig information ska ges vid ikryssande av samtyckesruta gällande
  - Personuppgiftsansvarig
  - Syfte med behandlingen
  - Övrig info kan lämnas på annan plats
- Om personuppgiftsbiträde byts ut krävs nytt samtycke
- Personuppgiftsbiträden måste anges

Rättslig förpliktelse

- Krav enligt lag att spara vissa uppgifter
  - Bokföringen
  - Skadeståndsmål

Intresseavvägning

- Intresseavvägning kan användas tillsammans med t ex avtal
- Kundrelation
- Medlemsrelation
- Förmånserbjudanden
- Säkerställa identifikation
  - I vissa fall får personnummer användas

Missbruksregeln

- Om missbruksregeln tidigare har använts måste man ta fram nya rutiner och instruktioner för ostrukturerad text såsom
  - Webbpublicering
  - Mail med personuppgifter
  - Nersparanden på datorn
- Detta kräver
  - Ny rättslig grund
  - Information till berörd
  - Register över behandlingen

Stärkta rättigheter

- Dataskyddsförordningen innebär framförallt stärkta rättigheter för den registrerades rätt
  - Att få tillgång till uppgifter
  - Till rättelse
  - Att bli glömd
  - Till begränsning av behandling
  - Till utförligare och tydligare information
  - Till portabilitet
  - Att göra invändningar mot direktmarknadsföring, profilering
  - Att informeras om anmälansmöjlighet

Faran med att göra fel

- Varumärket
- Sanktionsavgifter
  - Kompletterar varning, reprimand och föreläggande
- Skadestånd

- Skyldighet att informera om att de registrerade kan anmäla till Datainspektionen
- Är organisationen redo för en tillsyn?
- 1,2 miljoner tillsynsobjekt för Datainspektionen

Sanktioner

- Kännbara administrativa sanktioner införs
- Upp till den högsta summan av
  - 4 % av total årsomsättning, alternativt
  - 20 miljoner Euro
  - 2 % av total årsomsättning, alternativt
  - 10 miljoner Euro

Säkerhet

- Var och hur förvaras utrustningen?
  - Tillträde till lokaler
- Vem har tillgång till vad?
  - Behörighetstilldelning
- Var används mobila enheter?
  - Tas mobiler med till tredje land?
  - Arbetar man på caféer eller på tåget?
- Var sparas information?
  - Moln eller källaren?

Säkerhet

- Hur skickas information?
  - E-post med personuppgifter bör krypteras
- Loggar och historik
  - *När* har
  - *vem* gjort
  - *vad* med
  - *vilka* uppgifter och
  - *varför* har det gjorts
- Att läsa är att behandla

PAUS

Vad behöver göras?

- Utse en ansvarig för personuppgiftsfrågor
- Fastställ laglig grund
- Dokumentera och skapa rutiner
- Se över behörigheter
- Inventera, gallra och uppdatera
- Informera
- Se över information på hemsidan, sociala medier
- Skriv avtal med partners

Personuppgiftsansvarig

- Personuppgiftsansvarig är den som bestämmer ändamål och medel för behandlingen
- Ändamål och medel framgår troligen av anläggningsbeslutet

- Vem har ansvaret hos er?

Rättslig grund för registrering

- **Behandlingen är nödvändig för**
  - **Avtal**
  - **Rättslig förpliktelse**
  - Grundläggande intressen
  - Uppgift av allmänt intresse
  - Myndighetsutövning
  - **Intresseavvägning**
- **Samtycke**
- **Missbruksregeln försvinner**

Dokumentation och rutiner

- Dokumentera laglig grund
- Se över ändamål
- Skapa registerförteckningar
- Skapa skriftliga rutiner
- Rutiner måste följa även andra lagar

Behörigheter

- Vem ansvarar för vad?
- Vem tilldelar behörighet?
- Skapa rutiner att lägga till och ta bort
- Dokumentera behörigheter

Inventera

- Var finns personuppgifter?
- Vilka personuppgifter finns?
- För vilket ändamål sparas uppgifter?
- Är uppgifterna nödvändiga?
- Är uppgifterna aktuella?
- Vem har tillgång?

Gallra och uppdatera

- Ta bort inaktuella uppgifter
- Ta bort uppgifter som saknar laglig grund
- Rätta felaktiga och gamla uppgifter
- Tänk minimalism

Men, släng inte allt nu!!

Informera

- Berätta för medlemmarna vad ni har och varför
- Ge information om deras rättigheter
- Var alltid öppen
- Skaffa rutin för registerutdrag

- Informera om rätten att gå till tillsynsmyndighet

Hemsida och social media

- Se över all information som finns publicerad
- Skriv in ansvarig utgivare
- Utse en ansvarig för uppdatering

- Samma översyn behöver göras av information
  - På informationstavlor
  - På intern-TV
  - I gemensamma lokaler

Personuppgift, exempel

- Namn
- Adress
- Fastighetsbeteckning
- Telefonnummer
- Personnummer
- E-postadress
- Bilars registreringsnummer
- Fotografier och filmer

Personuppgift, exempel

- Namnlistor på event, anmälningslistor
- Tävlingsbidrag
- Protokoll från möten, om personuppgifter anges
- Foton från event
- Medlemsmatrikel
- Lista med registreringsnummer på bilar
- Debiteringslängd

Personuppgiftsbehandling

- Anteckningar
- Spar på egen dator eller telefon
- E-post
- Protokoll
- Att titta är att behandla

- Undantag
  - Data som privatperson lagrar för privat bruk

    Märk dock att jobbspar på privat telefon berörs av GDPR

Personuppgiftsbiträdesavtal

- Personuppgiftsbiträdesavtal ska tecknas
- Skriftligt avtal som nås i elektronisk form
- Ska komplettera tjänsteavtal

Konsulttjänster

- Tjänsteavtal
- Biträdesavtal
- Rutin för leverans av personuppgifter
- Rutin för hantering efter utförd tjänst

- Skicka inte adressfiler via e-post

E-postrutiner

- Skicka inte e-post till många
- Ta bort e-post i både in- och utkorg när det inte längre finns skäl att spara
- Tänk på att spara e-post så att de finns tillgängliga vid fråga om registerutdrag
- Fundera på hur du skriver i e-post, eftersom dessa kan krävas ut
- Skojiga händelser…

Fritext

- Missbruksregeln försvinner
- Tänk på hur du uttrycker dig i all text
- Vad kan publiceras
- Allt ska kunna lämnas ut

- Viktigt att samla allt på ett ställe och på ett sätt som tål att lämnas ut.

E-post och SMS

- Uppgifter får inte hämtas var som helst
- Får inte användas utan samtycke
- Enligt marknadsföringslagen får man inte skicka SMS eller e-post till personer man inte i förväg fått godkännande från

Facebook

- Publicera endast personuppgifter som ni har tillåtelse för genom t ex aktivt samtycke
- Måste synas varje dag
- Facebook är ett amerikanskt bolag

Foton och filmer

- Följer inte av medlemskapet att använda
- Skaffa skriftligt samtycke för att publicera bild
- Mall kommer att tas fram

- Använd inte samma bilder för länge, ett samtycke kan återkallas
- Se till att bilderna är aktuella
- T ex rätt styrelse på bilden på hemsidan

Anmälningslistor, tävlingsbidrag

- Upplys på blanketten vad uppgifter ska användas till
- Skaffa gallringsrutin för namnlistor
- Håll publicering av tävlingsvinster aktuella

- Fundera på varför listor m m finns, då kanske ni inser att de är onödiga att spara
- Aldrig tillåtet att spara ”Bra-ha-uppgifter”

Sjukfrånvaro

- Rutiner för sjukfrånvaro
  - Vad skrivs?
  - Var skrivs det?
  - Vem får info?
  - Vad meddelas i autosvar och på telefonsvarare

Tredje land

- All hantering av data ska skötas inom EU

- Överföring innebär inte bara lagring i moln
- Att ta med sig telefon och dator utanför EU innebär överföring av data till tredje land