GDPR – NY LAG OM BEHANDLING AV PERSONUPPGIFTER

Kerstin Wardman, 25 april 2018

SBAB!

Agenda

- Syfte och bakgrund med GDPR
- Exempel på stärkta rättigheter och skyldigheter
- Grundläggande begrepp
- Vad är en personuppgift?
- Principer för personuppgiftsbehandling
- Villkor för samtycke
- Ostrukturerad data – samma regler för all personuppgiftsbehandling!
- Kort tid kvar – vad behöver föreningen göra?
- Läs mer – länkar till bra och tydlig GDPR-information!

SBAB!

Syfte – varför nya regler?

- Dagens personuppgiftslag är från 1998 – omodern

- Syfte med den nya reglerna
  - uppdatera reglerna till dagens förutsättningar; internet, molntjänster, sociala nätverk
  - striktare integritetsregler
  - lika regler i alla EU-länder

- Harmoniserade regler är viktigt för
  - fria flödet av data
  - handel över landsgränser
  - skapar förtroende/säkerhet på internet

- Förordningen blir *direkt* tillämplig – behöver ej genomföras i nationell rätt

Exempel på stärkta rättigheter och skyldigheter

Stärkta rättigheter för de registrerade

- Lättare att få insyn
- Rätt att bli bortglömd
- Uppgiftsportabilitet

Tuffare krav för företag

- Tydligare utformning av samtycken
- Ökade krav på informationssäkerhet
- Rapportering av personuppgiftsincidenter
- Registerföring
- Undantag i PuL för ostrukturerad data försvinner
- Krav på dataskyddsombud
- Sanktioner

SBAB!

Grundläggande begrepp

- Personuppgiftsbehandling
  - varje åtgärd som, helt eller delvis automatiserat, vidtas med personuppgifter. T ex lagring, bearbetning, spridning, åtkomst etc

- Personuppgiftsansvarig
  - den organisation som bestämmer ändamålen och medlen för behandlingen av personuppgifter (t ex bostadsrättsföreningen)

- Personuppgiftsbiträde
  - den organisation som behandlar personuppgifter för den personuppgiftsansvariges räkning (t ex ekonomisk förvaltare, molntjänstleverantör)

- Dataskyddsombud
  - fysisk person som ska övervaka efterlevnaden av förordningen, informera och ge råd m m

SBAB!

Vad är en personuppgift?

- All slags information som antingen direkt eller indirekt kan kopplas till en fysisk person

- Känsliga personuppgifter får som huvudregel inte behandlas utan samtycke:

  - etniskt ursprung
  - politiska åsikter
  - religiös eller filosofiska övertygelse
  - medlemskap i fackförening
  - hälsa eller sexualliv eller sexuell läggning
  (t ex uppgift om handikappanpassat boende)
  - genetiska uppgifter (t ex foton)
  - biometriska uppgifter (t ex DNA)

EXEMPEL
- namn, personnummer
- enskild firma
- registreringsnummer fordon
- kundnummer
- lägenhetsnummer
- adress
- fastighetsbeteckning
- beteenden och preferenser
- krypterade uppgifter
- IP-nummer
- foton

SBAB!

Laglig behandling av personuppgifter

a) samtycke
t ex vid insamling av e-postadresser

eller nödvändig behandling för

b) att fullgöra avtal

c) rättslig förpliktelse
t ex skyldighet för brf-styrelse att föra medlems- och lägenhetsförteckningar enligt 9 kap. bostadsrättslagen

d) skydda intressen som är av grundläggande betydelse för den registrerade

e) arbetsuppgift av allmänt intresse eller led i myndighetsutövning

f) intresseavvägning

SBAB!

Principer för behandling av personuppgifter

a) laglighet, korrekthet och öppenhet

b) ändamålsbegränsning (särskilda, uttryckligt angivna och berättigade ändamål, ej behandla för oförenliga ändamål)

t ex ändamål medlemsförteckning = ge föreningen, medlemmarna och andra underlag för att bedöma medlemsförhållandena i föreningen

c) uppgiftsminimering (adekvata, relevanta, ej för många)

d) korrekthet (korrekta, uppdaterade, rättas utan dröjsmål)

e) lagringsminimering (ej spara längre än nödvändigt)

t ex medlemsförteckningen ska bevaras sju år efter föreningens upplösning (3 kap. Lag om ekon. föreningar)

f) integritet och konfidentialitet (uppgifterna ska skyddas mot obehörig eller otillåten behandling m m

SBAB!

Villkor för samtycke

- Formkrav
  - måste finnas innan behandlingen påbörjas
  - ej krav på skriftlighet
  - kan återkallas

- Frivilligt
  - fritt val för den enskilde, får ej villkoras

- Särskilt och otvetydigt
  - ett eller flera preciserade ändamål
  - kan komma till uttryck genom konkludent handlande

- Individuellt
  - en förening kan till exempel inte samtycka för sina medlemmars räkning

Ej godtagbara samtycken
- Tyst samtycke
- Hypotetiska samtycken
- Generella samtycken

SBAB!

Samma regler för all personuppgiftsbehandling

- Undantagsregeln för personuppgifter i ostrukturerat material försvinner 25 maj 2018
  - e-post
  - löpande text på internet
  - fritextfält

- Alla företag i Sverige har en ”backlog”
  - undantag för ostrukturerat material unik regel för Sverige

- Hela dataskyddsförordningen gäller för alla personuppgifter, vilket innebär att man ska…
  - följa de grundläggande principerna
  - ha en rättslig grund för behandlingen
  - ha en förteckning över personuppgiftsbehandlingar
  - informera om personuppgiftsbehandlingen
  - ha rutiner för att hantera en begäran om att lämna ut eller radera personuppgifter
  - skydda personuppgifterna (informationssäkerhet)

SBAB!

Vad behöver föreningen göra?

- Informera alla i styrelsen om vad GDPR innebär och vad som kommer att gälla
  - även om förvaltare anlitas

- Inventera
  - vilka register förs och på vilken laglig grund?
  - varifrån hämtas personuppgifterna?
  - gallring; raderas inaktuella register?

- Inhämta samtycke
  - t ex för publicering av namn, e-postadresser, bilder etc på föreningens webbplats
  - insamling av e-postadresser
  - granska befintliga samtycken
  - aktivt samtycke efter tydlig information; använd gärna kryss- eller klickrutor

- Information till registrerade
  - se över rutiner för hur personuppgifter lämnas ut på begäran (registerutdrag)

SBAB!

Läs mer

- Datainspektionens hemsida
  https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/

- Bostadsrätternas GDPR-guide
  http://www.bostadsratterna.se/allt-om-bostadsratt/artiklar/gdpr-guide-till-de-nya-reglerna

- **Fastighetsägarnas information ”Förberedelser inför GDPR”**
  http://www.fastighetsagarna.se/kunskapsbanken/juridik-avtal-och-overenskommelser/personuppgiftshantering-och-gdpr

- GDPR-guide för småföretagare
  https://www.verksamt.se/driva/gdpr-dataskyddsregler/gdpr-guiden

- Dataskyddsförordningens i sin helhet
  http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=SV

SBAB!