

[info hämtad från <https://foreningsresursen.fi>]

GDPR - EU:s dataskyddsreform

GDPR eller General Data Protection Regulation är EU:s nya allmänna dataskyddförordning. Förordningen antogs 2016 och träder i kraft i hela EU den 25 maj 2018 och ersätter nationell register- och personuppgiftslagstiftning.

De nya reglerna medför förändringar som också påverkar föreningar. Alla föreningar är skyldiga att upprätthålla medlemsregister och berörs därför direkt av reformen. Föreningar som endast har organisationer som medlemmar berörs inte beträffande medlemsregistret, men behandlar givetvis i andra sammanhang personuppgifter.

GDPR är en omfattande och komplicerad helhet och det är viktigt att åtminstone i huvuddrag sätta sig in i reglerna.

Bakgrund

Data i olika former och särskilt data som gäller enskilda personer är framtidens guld eller olja. Med exakta uppgifter om individer; intressen, personlighet, hälsotillstånd och så vidare, är det möjligt att utveckla och skraddarsy nya produkter och tjänster. Idag är det självklart att mobiltelefoner, bilar, tv-apparater och datorer ständigt är uppkopplade och registrerar information om hur de används. I framtiden väntas alltfler om inte de flesta tekniska apparater, allt från brödrostar till kylskåp, producera data om hur de används.

GDPR är ett försök att reglera hur data som gäller enskilda individer får behandlas inom EU. Förordningen syftar till att införa ett nytt tänkande där en central idé är att säkerställa den enskilda individens möjlighet till kontroll över sina egna personuppgifter. För organisationer som hanterar personuppgifter räcker det inte längre att passivt följa regler utan de måste nu aktivt kunna påvisa att de uppfyller reglerna. Juridiskt sett är det frågan om ett paradigmskifte. Artikel 5 slår fast att "den personuppgiftsansvarige ska ansvara för och kunna visa att principerna efterlevs". De nya reglerna ger också de övervakande myndigheterna möjlighet till administrativa sanktionsavgifter. För allvariga överträdelser kan företag påföras avgifter på upp till 4 procent av den globala omsättningen, för övriga kan avgiften vara upp till 20 000 000 €.

Berättigade ändamål

I förordningen stadgas att behandling av personuppgifter är laglig endast om och i den mån som minst ett av de villkor som uttryckligen nämns uppfylls. Av de sex berättigade ändamål som nämns är några omedelbart relevanta för föreningar. För det första sägs att behandling är laglig i fall den är nödvändig för att fullgöra en rättslig förpliktelse, som åvilar den personuppgiftsansvarige. Föreningslagen förutsätter att alla föreningar upprätthåller en förteckning över sina medlemmar. Ett annat alternativ är regeln att behandlingen är laglig om den registrerade har lämnat

sitt samtycke till behandling för ett eller flera specifika ändamål. Samtycket skall dock kunna påvisas av den som behandlar personuppgifterna och det kan under den här regeln när som helst återtå. Att hantera samtycke kan i praktiken vara arbetsdrygt för en mindre förening. Det tredje alternativet är den allmänna regeln att behandling är laglig i fall den är nödvändig för ändamål som berör den personuppgiftsansvariges berättigade intressen. Det här begreppet definieras inte närmare och det är alltså upp till den som behandlar uppgifterna att visa att behovet av behandlingen väger tyngre än den registrerades rättigheter. För föreningar lönar det sig alltså att se till att behandlingen så långt som möjligt grundar sig på regeln om rättsliga förpliktelser.

Principer

Förordningen anger en uppsättning principer som alltid skall iakttas då personuppgifter behandlas. Det är inte möjligt att utförligt behandla de olika principer som förordningen anger för behandlingen av personuppgifter i denna korta artikel. Den övergripande tanken är ändå att behandlingen skall bygga på tydliga behov, att uppgifter endast får användas för det syfte de har samlats in för, att inga onödiga eller alltför omfattande uppgifter får samlas in, att uppgifterna inte får behandlas under längre tid än de behövs för och att dataskyddet skall vara tillräckligt starkt.

Rättigheter

De nya bestämmelserna anger att den registrerade har en uppsättning rättigheter. Som med principerna är det inte möjligt att gå igenom rättigheterna i detalj. Den registrerade har bland annat rätt till tillgång, rätt till rättelse och rätt till radering under vissa förutsättningar. Begreppet "registerbeskrivning" finns inte med i de nya bestämmelserna, men i stället nämns en uppsättning information som skall ges till den registrerade när personuppgifterna tas emot. Detta framgår i artikel 13. Har man ett register skall man alltså när man tar emot personuppgifter i framtiden till den man tar emot den av lämna den information som nämns i artikel 13.

Hur förbereda sig?

Varje förening ska börja med att utreda vilka personuppgifter den behandlar och i vilka sammanhang det sker. Medlemsregistret är knappast det enda sammanhanget där personuppgifter behandlas i en förening. Skapa en kortfattad översikt eller processbeskrivning av nuläget. Utred sedan den rättsliga grunden för de olika sammanhang som personuppgifter behandlas inom. Fastställ sedan 1) hur föreningen påvisar att den följer principerna för behandling av personuppgifter och 2) hur föreningen garanterar den registrerades rättigheter. Till det hör att skapa den information enligt artikel 13 som behövs. Se till att dokumentera hela det här arbetet skriftligt - det behöver inte vara en lång litanja, några A4:or ska räcka för en vanlig liten förening - och ta upp det i styrelsen så att det blir protokollfört.