SVERAK och Dataskyddsförordningen

25 maj - GDPR - General Data Protection Regulation

Vad innebär GDPR och gäller den oss?

Den 25 maj 2018 träder den nya dataskyddsförordningen i kraft, den innebär gemensamma regler i EU/EES och den gäller för alla, små som stora organisationer som hanterar data om EU-medborgare. Man kan säga att utgångspunkten är att det är förbjudet att hantera personuppgifter, men att det finns undantag som beskrivs i GDPR.

GDPR ersätter PUL och ställer strängare krav på personuppgiftshantering än vad PUL gjort. Genom GDPR får privatpersoner starkare rätt att förfoga över sina personuppgifter och att invända mot hur företag och organisationer använder uppgifterna.

Syftet med insamling av personuppgifter ska anges. Det omfattar även var data lagras, vilka som har tillgång till data, med vilka tredje parter data utbyts och var de håller till. Organisationen ska kunna redovisa varifrån uppgiften kommer, vad den ska användas till och tillse att den är korrekt och aktuell.

Personen som personuppgifterna gäller har rätt att få insyn i uppgifterna som lagras och begära ändringar/korrigeringar, liksom att i de flesta fall få uppgifterna raderade.

GDPR gör ingen skillnad på strukturerade och ostrukturerade personuppgifter. Det innebär att e-post, dokument, bilder och videor omfattas av GDPR. GDPR är också teknikneutral, vilket innebär att den även gäller för uppgifter på papper. All information som direkt eller indirekt kan identifiera en fysisk person är hantering av personuppgifter, t.ex. att nämna en persons namn i en e-post.

Datasäkerhet ska byggas in i systemen som behandlar personuppgifter och lämpliga organisatoriska och tekniska åtgärder ska vidtas för att säkerställa lämplig säkerhet i förhållande till risken. En riskanalys av systemen ska göras. Datasäkerhetskraven innebär att personuppgifter inte får komma i orätta händer och att förlust av data ska anmälas till Datainspektionen (DI) och till personer som omfattas av datauppgifterna.

Att inte uppfylla reglerna kan leda till omfattande böter. Här finns inga undantag (än så länge), vilket kan innebära allvarliga konsekvenser för små föreningar med begränsade ekonomiska resurser.

Datainspektionen (DI) kommer att få nya verktyg för att tillse att förordningen följs; varning, reprimand och sanktionsavgift. Avgiften är upp till 20 miljoner euro eller 4% av den globala omsättningen (beroende på överträdelse). Det kommer även finnas möjlighet för enskilda att begära skadestånd vid överträdelser.

Ordförklaring

- **Personuppgift:** All data som kan användas för att identifiera en fysisk person. T.ex. namn, adress, personnummer, e-postadress, en katts registrerings- och ID-nummer, osv.
- **Personuppgiftsregister:** En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier. Medlemsregister, e-postistor, utställningskataloger, osv.
- **Personuppgiftsansvarig:** En fysisk person eller en organisation (t.ex. SVERAK eller ansluten kattklubb) som registret har skapats för och som bestämmer hur uppgifterna i registret ska användas. Det är föreningen som är personuppgiftsansvarig och styrelsen som ansvarar för att föreningen följer lagen, detta oavsett om det finns ett dataskyddsombud eller om föreningen t.ex. utsett någon som är ansvarig för medlemslistor.
- **Personuppgiftsbiträde:** En fysisk person, offentlig myndighet eller annat organ som behandlar personuppgiftsregistret för en personuppgiftsansvarigs räkning enligt hans eller hennes instruktion. Till exempel leverantör av verktyg för e-postmarknadsföring.
- **Dataskyddsombud:** En fysisk person som övervakar att organisationen följer dataskyddsförordningen. Till uppgifterna hör att kontrollera organisationens efterföljande av förordningen, informera och fungera som kontaktperson i personuppgiftsfrågor.
- **Laglig grund:** Med vilket stöd i förordningen man samlar in och lagrar personuppgifter.

De lagliga grunder som är mest aktuella är:

- **Samtycke** – Man frågar och får lov. Gäller t ex viss marknadsföring. Man måste få information först och sen uttrycklig godkänna, t.ex. godtas inte ett tyst samtycke eller en på förhand ikryssad ruta på en webbplats. Man måste i efterhand kunna visa att samtycke har lämnats och att samtycket uppfyller kraven i förordningen. Om så inte är fallet, måste man antingen förändra sina rutiner eller finna en annan rättslig grund för behandlingen.
- **Avtal** – Föreningens stadgar kan ses som ett avtal med medlemmarna. Den vanliga medlemshanteringen baseras alltså på avtal. Vill man inte att föreningen ska behandla personuppgifterna, så kan man t.ex. inte bli/vara medlem eller delta på utställningen.
- **Lag** – När det finns ett rättsligt krav att behandla personuppgifter, t. ex. skattelagstiftning, LAS, bokföringsskyldighet, osv.
- **Intresseavvägning** – Personuppgifter kan också få behandlas om föreningens intresse att få behandla personuppgifterna väger tyngre än intrånget i den enskildes integritet. I denna del finns ingen större skillnad mellan GDPR och PUL.

- Det är inte ovanligt att organisationer anser sig ha flera alternativa grunder för sin behandling.
- Genom dataskyddsförordningen införs ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk. Kort sagt, om man erbjuder den typen av tjänster till barn under 16 år måste man inhämta vårdnadshavares samtycke för att få behandla barnets uppgifter (åldern kan sättas ned till 13 år av medlemsländerna). Kom ihåg att man då också måste kunna visa att vårdnadshavarens samtycke har lämnats.

När GDPR börjar gälla måste vi ha följande rutiner på plats:

- Veta vilka personuppgifter vi har.
- Klarlagt grunden för varför vi har personuppgifterna.
- Säkerställa personuppgifternas korrekthet, aktualitet och relevans.
- Ta fram alla personuppgifter om en person när denne så begär.
- Kunna radera alla personuppgifter på begäran (om inga hinder föreligger).
- Ändra/korrigera personuppgifter.
- Informera andra organisationer om ändringar i de fall personuppgifterna överförts till andra.
- Om vi tagit emot personuppgifter från andra organisationer skall vi kunna korrigera och radera uppgifterna på begäran.
- Inhämta samtycke från dem vi samlar in personuppgifter om.
- Kontrollera åldern på personer som lämnar personuppgifter.
- Informera om vad personuppgifterna skall användas till och med vilken rätt de samlats in, liksom vilka rättigheter den registrerade har enligt GDPR.
- Säkerställa datasäkerheten.
- Vid säkerhetsincidenter rapportera till Datainspektionen inom föreskriven tid (72 timmar), liksom att informera berörda.
- Veta hur uppgifter behandlas vid överföring av personuppgifter till länder utanför EU/EES. (T.ex. server utanför EU/EES)

Hur gör vi för att uppfylla allt detta?

- Kartlägg behandling
- Laglig grund för behandlingen
- Se över rutiner
- Kontrollera säkerhet på datasystem
- Gå igenom/upprätta dokumentation
- Utse dataskyddsombud

Kartläggning - Riskanalys

Vilka personuppgifter behandlar vi; behövs alla uppgifter och varför? För föreningens del handlar detta främst om att se över vilka data som lagras om nuvarande och tidigare medlemmar och förtroendevalda. Lagras känslig data?

Hur behandlar vi personuppgifter, var lagras uppgifterna och hur ser datasäkerheten ut? I denna del handlar det om att se över sina databaser/tjänster för medlemsregister, e-post, nyhetsbrev, osv.

Vem har tillgång till personuppgifterna och varför? Gör en genomgång av vilka i föreningen som har tillgång och anledningen till varför dessa personer måste ha tillgång till uppgifterna. Vilka utomstående aktörer kan få ta del av uppgifterna?

Vad händer med gamla personuppgifter och vad gör vi om någon begär att få ut uppgifter? Se över hur gammal data behandlas, vilka rutiner som finns för att lämna ut, ändra och radera uppgifter. Hur informeras medlemmarna om lagringen?

Känsliga data – inte behandlar vi sådana?

Jo, det kanske ni gör. Lagen definierar en viss sorts personuppgifter som känsliga. Till exempel uppgifter om en persons hälsa (inbegripet funktionsnedsättning), religiös, politisk eller filosofisk övertygelse, etnicitet, fackligt medlemskap m.m. Sådana uppgifter får i princip bara behandlas med den registrerades samtycke.

När behandlar vi såna uppgifter? T.ex. vid årsmöten då man samlar in information om allergier i samband med matbeställning. Ta med information om detta i ert policydokument. Grunden för behandling är frivilligt utlämnande vilket är att anse som ett giltigt samtycke.

Behandling av personnummer regleras av medlemsländerna själva och DI har för Sveriges del bestämt att sådan data får behandlas om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. OBS. Som laglig grund för behandlingen av personnummer kan man inte ange intresseavvägning.

Rutiner för behandling av personuppgifter

- Rutiner för att införa och kontinuerligt se över registerförteckning på alla behandlingar.
- Säkerställ så det endast är personer som behöver tillgång som har det. Ändra lösenord vid behov. Ha rutiner för hur detta hanteras, t.ex. vid byte av förtroendevalda.
- Utarbeta rutiner för utlämnande, rättning och radering både i eget register och andras (dit man överfört uppgifter, t.ex SVERAK).
- Vilka rutiner finns vid arkivering?
- Inför rutiner för hur samtycke ska inhämtas och hur samtycket ska sparas. Dokumentera i vilka sammanhang det kan vara aktuellt med samtycke.
- Upprätta rutiner för att informera om insamlandet av personuppgifter och kontrollera så lagens krav på vilken information som ska ges är uppfyllt.
- Rutin för att upptäcka, utreda och rapportera incidenter som riskerar fysiska personers rättigheter och friheter. Vem ansvarar för att göra en sådan anmälan inom tidsfristen?
- Rutin för kontinuerlig översyn, arbetet är aldrig färdigt. Sätt upp GDPR - personuppgiftsskydd som en återkommande punkt på styrelsens dagordning. Redovisa i protokoll och i verksamhetsberättelsen hur arbetet med kontroller och förbättringar görs.

Datasäkerhet

Kontrollera att personuppgifterna hanteras säkert.

Kanske finns behörighetssystem eller kryptering som borde användas. Om medlemslistor skickas med e-post bör man söka en annan lösning; e-post är närmast jämförbar med vykort. Kartlägg hur databaser och fysiska enheter är kopplade.

Leverantörer och avtal – personuppgiftsbiträdesavtal.

När man vet vilka system man använder så ska man teckna avtal med alla sina biträden. Om man använder en ”molntjänst” så ska man ha biträdesavtal med leverantören, många leverantörer har redan detta på plats och man kanske redan har ingått ett avtal genom att acceptera uppdaterade villkor.

Servermiljö

Lagrar ni personuppgifterna på egna servrar, i ett serverhotell eller i en molntjänst? Finns uppgifterna lagrade i Sverige eller utomlands? Användandet av populära molntjänster som Google Drive, Dropbox, etc. innebär i många fall överföring av personuppgifter till tredje land (USA räknas som tredje land). I så fall måste den registrerade informeras om detta. Sådan överföring är bara tillåten om landet eller företaget som personuppgifterna överförs till anses ha en adekvat skyddsnivå eller om ni som organisation vidtagit skyddsåtgärder.

Dokumentation - Den kanske viktigaste delen i GDPR

- **Intern policy för dataskydd**

Dokumentera vad ni kommit fram till under kartläggningen och de rutiner ni har/har skapat för att visa föreningens efterlevnad av GDPR. Ange hur föreningen arbetar med att uppfylla kraven; vad som händer om en begäran om rättning, överföring, radering, osv görs.

- **Registerförteckning**

GDPR kräver att man kan uppvisa en förteckning över vilka register som behandlar personuppgifter som föreningen hanterar, vem som har tillgång till dem, varför registret förs och vilka uppgifter om enskilda som behandlas i registren. T.ex. medlemsregister, innehåller namn, adress och e-postadress till medlemmar, lagras enligt avtal om medlemskap, hanteras av XX. Lämnas registret ut till tredje part är det viktigt att ange även det.

- **Rutinbeskrivningar**

Dokumentationen kan behöva kompletteras med rutinbeskrivningar om hur man hanterar uppgifter som ännu inte hamnat i något register. T.ex. om man samlar in namnunderskrifter manuellt.

- **Integritetspolicy**

Upprättas för att informera enskilda om hur behandling av deras personuppgifter görs och hur de kan ta del av, ändra och ta bort informationen som lagras om dem. Denna policy ska var lättillgänglig på webbsida, Facebook, osv.

- **Tänk på att:**

Laglig grund för behandling av personuppgifterna ska framgå av all dokumentation.

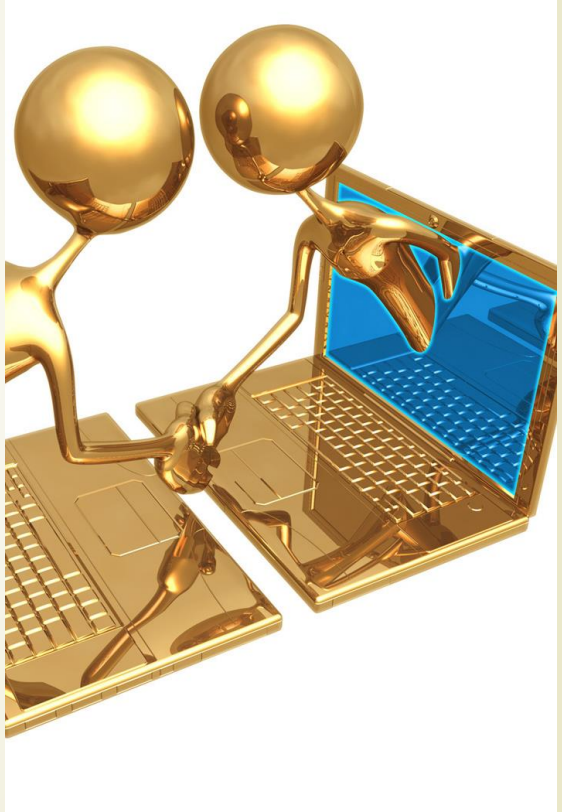
Dokumentationen ska föras elektroniskt och på begäran kunna tillställas Datainspektionen.

Transparens

Kravet på transparens i GDPR innebär bland annat att de registrerade har rätt att känna till vilka personuppgifter om dem som behandlas. Föreningen måste därför bland annat se till att informera de registrerade om att deras personuppgifter behandlas och för vilka ändamål, vilka rättigheter de har gentemot föreningen och så vidare. Denna information måste lämnas i samband med att personuppgifterna samlas in.

Transparenskravet innebär också att de registrerade har rätt att på begäran få registerutdrag, det vill säga information från föreningen om vilka personuppgifter som behandlas om dem, samt få sina uppgifter överförda till annan organisation.

Man har också rätt att få information om hur man ändrar och begär radering av sina uppgifter och när det kan ske.



Dataskyddsombud

- Måste vi utse ett dataskyddsombud?
- NEJ! Ett måste bara för:
  - Organisationer inom offentlig sektor
  - Företag med fler än 250 anställda
  - Organisation som i sin verksamhet behandlar känsliga uppgifter eller stora register.

- Kan vi utse ett dataskyddsombud?
- Självklart!
  - Även om ni inte måste ha ett dataskyddsombud kan det vara bra att ha ett för att skapa ordning och reda i arbetet med personuppgifter. Det kan också skapa förtroende hos de registrerade.
  - Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen.

Kom ihåg!

- Om behandling av personuppgifter kan leda till en hög risk för enskilda personers fri- och rättigheter ska man alltid göra en konsekvensbedömning. Detta kan man läsa mer om hos DI
- Det är föreningen/styrelsen som är ansvariga för hanteringen, aldrig en enskild.
- Ni ”lånar” personuppgifter, hantera dem varsamt och bara så länge det behövs.
- En registerförteckning och policydokument ska upprättas, exempel att utgå från kommer finnas på SVERAKs hemsida.
- Det är inte så krångligt som det låter. Era policydokument och upprättade rutiner kommer ta hand om det mesta.
- SVERAK finns alltid till hands att fråga om ni är i tvivel om vad som gäller.

Sammanfattningsvis…

Att dokumentera sitt arbete med att följa GDPR blir oerhört viktigt. Som personuppgiftsansvarig har man bevisbördan för att lagen följs. Kan man inte visa det med dokumentation så är det i sig ett lagbrott.

Sådär! Då är vi färdiga!
Då behöver vi väl inte göra nåt mer?

Fel!

Arbetet är kontinuerligt och måste ständigt ses över. Uppföljningar ska göras regelbundet och det ska visas i dokumentationen. Man kan alltså inte ”bli färdig” med sitt GDPR-arbete utan man måste ha koll på att skyddet upprätthålls hela tiden.

Utbilda, informera och uppdatera. Tänk integritet!