Stockholm den 23 mars 2018

SENIORERNA

Integritet – dataskydd och personuppgifter

Den 25 maj 2018 börjar nya bestämmelser gälla för skyddet av personuppgifter. Då ersätts personuppgiftslagen (PuL) med dataskyddsförordningen (ibland används den engelska förkortningen *GDPR, General Data Protection Regulation*). De nya bestämmelserna ger oss anledning att påminna om integritets- och dataskydd, se över rutiner för hantering av personuppgifter, samt ger möjlighet till förbättringar.

Personuppgift = allt som kan kopplas till en fysisk person

All slags information som direkt eller indirekt kan hänföras till en viss fysisk person som är i livet räknas som personuppgifter. Även fotografier, bilder och ljudupp-tagningar på individer som kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.

Behandling av personuppgifter = allt som görs med dem

Med behandling av personuppgifter menas allt man gör med dem – all hantering av personuppgifter. Exempel på behandling av personuppgifter är insamling, registrering, lagring, sortering, bearbetning och spridning.

Inventera, analysera, dokumentera

Inför att de nya bestämmelserna börjar gälla är det bra för alla organisationsled - föreningar, distrikt och förbund – och deras styrelser att se över sin behandling av personuppgifter.

1. **Inventering**
   Vilka personuppgifter har vi samlat, vilka behandlingar av dem sker och till vem lämnas de ut? Vilken information ger vi till registrerade, och räcker den?
   Till exempel har vi medlemsregister, löne- och personalregister, kurs- och konferensadministration, dokumentation från verksamhet och aktiviteter samt publicering på webbplats eller i annan löpande text samt fotografier.

2. **Analys**
   Vilka risker finns för att behandlingen av personuppgifter kan skada den registrerades integritet?

3. **Dokumentation**
   Dokumentera den genomförda kartläggningen och analysen, det vill säga sammanställ vilken typ av personuppgifter som behandlas och på vilket sätt och i vilka sammanhang personuppgifter behandlas.

SPF Seniorerna
Hantverkargatan 25, Box 225 74, 104 22 Stockholm
Tel 08-692 32 50 info@spfseniorerna.se
Org nr 88 80 00-2830 Pg 607678-0 Bg 5959-0182
www.spfseniorerna.se

Register och matriklar i föreningar och distrikt

Hantering av personuppgifter medför ett särskilt ansvar att behandla personuppgifterna försiktigt och med respekt för de registrerades personliga integritet. Insamling, lagring, sammanställning och varje annan behandling av personuppgifter fordrar antingen att man har uttryckligt stöd i lagen för varje specifik hantering av just de specifika personuppgifterna, eller att man har ett uttryckligt samtycke – stöd – från de person vars uppgifter det gäller.
Med hänvisning till detta avråder förbundet från lokala register med personuppgifter. Den förening eller distrikt som tar på sig en sådan uppgift blir personuppgiftsansvarig och tar därmed på sig ett stort ansvar.

För kunna sammanställa och sprida en medlemsmatrikel krävs att den som producerar matrikeln inhämtat samtycke från de personer som är tänkta att ingå i matrikeln. En person som inte samtyckt får inte ingå i matrikeln. Nya medlemmar i föreningen måste informeras om exakt vilka uppgifter om dem som kan komma att spridas i en medlemsmatrikel och de måste samtycka till just exakt de uppgifterna, och just exakt det spridningssättet (matrikel). De uppgifter och det sätt som medlemmen inte samtycker till får inte finnas med/spridas på det sättet.

Gällande rätt och nyheter

Det flesta bestämmelser som gäller i dag med personuppgiftslagen (PuL) kommer också att gälla under dataskyddsförordningen. Liksom tidigare ska man inte samla in fler personuppgifter än nödvändigt, inte ha kvar uppgifterna längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in.
Inom SPF Seniorerna finns ingen anledning att behandla personuppgifterna som är särskilt känsliga (ursprung, åsikter, övertygelse, fackföreningsmedlemskap, genetik, biometri, hälsa, sexualliv och sexuell läggning).
Personuppgifter ska vara korrekta och uppdaterade samt förvaras i en form som är säker och gör det möjligt för den registrerade att i rimlig tid identifiera sina egna uppgifter.

Den som samlar in, behandlar eller på annat sätt hanterar personuppgifter är i lagens mening personuppgiftsansvarig. Förbundet är personuppgiftsansvarigt för behandlingar av personuppgifter i det centrala medlemsregistret. Behandling av personuppgifter som föreningar och distrikt gör ansvar de för.

Den enskilde har rättigheter
En enskild person, i vårt fall typiskt sett en medlem, har redan i dag med rätt att

- få **information** om att behandling av personuppgifter kan ske eller pågår,
- få **utdrag** om vilka behandling av egna personuppgifter som sker,
  om uppgifterna behandlas för att uppfylla ett avtal eller om de behandlas med stöd av ett samtycke som personen har lämnat,

- få egna personuppgifter **raderade**, t.ex. för att hen motsätter sig direktmarknadsföring,
- få **skadestånd** – ersättning vid skada, samt
- **klaga** till Datainspektionen – myndigheten kan inleda tillsyn.

Genom dataskyddsförordningen får den enskilde dessutom rätt att
- få **rättelse** eller komplettering av felaktiga eller inkompletta personuppgifter, och
- överföra (**dataportabilitet**) personuppgifter som den registrerade själv har lämnat, till annan personuppgiftsansvarig, exempelvis annan organisation eller en social medietjänst (t.ex. Facebook, Twitter, Instagram) om den registrerade har lämnat samtycke och behandlingen sker automatiserat.

Enklare personuppgiftsbehandling
PuL ger i dag en möjlighet att behandla personuppgifter i ostrukturerat material. Behandling i ostrukturerat material är till exempel icke sökbara personuppgifter i databaser, listor och Excel på papper, publicering av personuppgifter på en webbplats eller i annan löpande text eller bild på internet. Enligt PuL krävs då inget samtycke från den vars personuppgifter det berör, så länge inte någons personliga integritet kränks. Dataskyddsförordning är, enligt lagtexten, teknikneutral. Det betyder att den inte tar hänsyn till om materialet är ostrukturerat eller inte. All hantering av personuppgifter, oavsett format, fordrar samma höga krav på försiktighet.

Tänka efter före
Inför varje personuppgiftsbehandling är det bra att bedöma risker för de registrerade, konsekvenser av behandlingen och åtgärder för att minska eventuella riskerna. Dataskyddsförordningen kräver att detta sker och dokumenteras om risken är hög för att registrerades fri- och rättigheter kränks eller om personuppgifterna är särskilt känsliga (ursprung, åsikter, övertygelse, fackföreningsmedlemskap, genetik, biometri, hälsa, sexualliv, sexuell läggning).

Säkerhetsincident
Den som brister i sin personuppgiftshantering kan orsaka en personuppgiftsincident. Det vill säga en händelse som äventyrar den registrerades integritet, genom att personuppgifter medvetet eller omedvetet förstörs, ändras, förloras eller den personuppgiftsansvariga (SPF Seniorerna) röjer uppgifterna för obehöriga.
Om säkerhetsincidenten är tillräckligt allvarlig ska den personuppgiftsansvariga (SPF Seniorerna) åtgärda felet, anmäla till Datainspektionen inom 72 timmar från upptäckten samt informera registrerade.
För säkerhetsincidenter kopplat till det centrala medlemsregistret ansvarar förbundet. Förbundet åtgärdar då felet, anmäler incidenten och informerar registrerade.
Om incidenten sker hos ett personuppgiftsbiträde (underleverantör till SPF Seniorerna) ska biträdet omedelbart rapportera till oss.
Misstänkta allvarliga personuppgiftsincidenter anmäls till förbundet via e-postadressen info@spfseniorerna.se

Sanktioner
Om den personuppgiftsansvariga (SPF Seniorerna) inte anmäler en personuppgiftsincident som ska anmälas, eller anmäler för sent, kan den personuppgiftsansvariga bli skyldig att betala en sanktionsavgift.

Andra åtgärder som Datainspektionen kommer att ha möjlighet till är att utfärda varning, reprimand, föreläggande samt begränsa och förbjuda behandling av personuppgifter.

Dataskyddsombud
Möjligheten att utse personuppgiftsombud försvinner. Istället ska personuppgiftsansvariga utse dataskyddsombud om de är offentliga organ eller om kärnverksamheten är att övervaka enskilda eller behandla personuppgifterna som är särskilt känsliga (ursprung, åsikter, övertygelse, fackföreningsmedlemskap, genetik, biometri, hälsa, sexualliv, sexuell läggning).
SPF Seniorernas föreningar, distrikt och förbundet behöver inte utse dataskyddsombud.

Överföring av uppgifter utanför EU och EES
Överföring av personuppgifter till länder utanför det europeiska ekonomiska samarbetsområdet (EES) får bara ske under särskilda förutsättningar efter godkännande av förbundet.

Datainspektionen och de andra EES-ländernas dataskyddsmyndigheter arbetar just nu med att ta fram en vägledning för överföring av personuppgifter utanför EU/EES.

Bakgrund – dataskyddsförordningen

Skälet till dataskyddsförordningen (och tidigare personuppgiftslagen) är att värna respekten för privat- och familjeliv samt personlig integritet. Dessa är grundläggande fri- och rättigheter i den europeiska unionen. Genom dataskyddsförordningen stärks skyddet i EU ytterligare.

Personuppgiftslagen (PuL) bygger på ett EU-direktiv, vilket betyder att varje medlemsstat genomförde det på sitt eget sätt. Det har lett till olika tillämpning av bestämmelserna, vilket missgynnar personer och företag som verkar över nationsgränserna. De nya bestämmelserna har beslutats i form av en EU-förordning, vilket betyder att den är direkt gällande i varje medlemsstat och inte får särskilt genomföras individuellt.

På Datainspektionens webbplats kan man läsa mer om dataskyddsbestämmelser:
https://www.datainspektionen.se/dataskyddsreformen/

Länk till dataskyddsförordningen på svenska:
https://www.datainspektionen.se/Documents/Dataskyddsförordningen%20-