Svenska Blå Stjärnan

Vad är dataskyddsförordningen – GDPR
Den 25 maj 2018 fick Sverige och övriga EU en ny gemensam lagstiftning som reglerar hur företag och organisationer får behandla personuppgifter. Dataskyddsförordningen som kallas för GDPR (General Data Protection Regulation) ersatte den svenska personuppgiftslagen (PuL). Alla verksamheter som behandlar personuppgifter omfattas av GDPR.
Dataskyddsförordningen ställer strängare krav på hur företag och organisationer får samla in och använda personuppgifter än PuL. Om man bryter mot reglerna i förordningen så riskerar man kännbara böter. Därför är det viktigt att känna till vilka regler som gäller när man använder personuppgifter.

Vem ansvarar för Svenska Blå Stjärnans personuppgifter?
Svenska Blå Stjärnans förbund och ungdomsförbund är egna juridiska personer. Det innebär att dessa är personuppgiftsansvariga för hanteringen av de egna medlemmarnas personuppgifter. Det är viktigt att tänka på hur personuppgifterna används, vad de används till och hur de lagras. Man måste också tänka på hur de är skyddade mot dataintrång.
Medlemsregister Rosa, som förbund och ungdomsavdelningar har tillgång till, är en del av det centrala medlemsregistret Ferdinand. Detta innebär att vi har ett delat ansvar att följa de regler som gäller för att säkra den personliga integriteten.

Vad är en personuppgift?
Personuppgifter är all slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Exempel på personuppgifter är personnummer, namn, adress och e-postadress och vissa typer av cookies och ip-adresser. Även foton på personer och ljudupptagningar som behandlas i datorn är personuppgifter.

Vad är en känslig personuppgift?
Känsliga personuppgifter är sådana uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, personuppgifter som rör hälsa eller sexualitet samt genetiska och biometriska uppgifter som entydigt identifierar en person.

Vad är ett personregister?
När man registrerar olika uppgifter om en enskild person som t.ex. personnamn, person-nummer, telefonnummer, e-postadress eller registreringsnummer på bilen så har man skapat ett personregister. Alla register där uppgifterna på ett eller annat sätt kan hänföras till en enskild individ är ett personregister. Det har ingen betydelse om det är ett papper i en pärm, en excelfil eller ett mejl. Detta innebär att t.ex. en namnlista på papper som upprättas inför ett studiebesök räknas som ett register och ska hanteras enligt GDPR.

Registerbeskrivning
För varje behandling av personuppgifter ska en registerbeskrivning upprättas. Det är viktigt att kunna uppge vilken information som behandlas, hur den behandlas och vilka rutiner man har vid en eventuell personuppgiftsincident.

Vad innebär GDPR?
GDPR har nästan dubbelt så många bestämmelser som PuL. Här följer några av de främsta förändringarna i och med införandet av GDPR.

1. Varje organisation ska utse en personuppgiftsansvarig
Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till). Det är alltså är inte chefen på en arbetsplats eller en anställd som är personuppgifts-ansvarig. Även en fysisk person kan vara personuppgiftsansvarig, vilket till exempel är fallet för enskilda firmor.

2. Förutom grundläggande dataskyddsprinciper så har kravet på uttryckligt medgivande skärpts.
* Aktivt medgivande krävs av individen, vilket innebär att man genom en frivillig handling, efter att ha blivit informerad om konsekvenserna, går med på att få sina personuppgifter behandlade. Ett samtycke måste alltid vara aktivt, frivilligt och individuellt.
* Medgivandet ska vara uttryckligt och klart. Uttryckligt samtycke innebär att den berörda klart och tydligt anger vad hon ger sitt samtycke till. Det bör vara mer precist beskrivande.
* Individer som berörs av hanteringen av personuppgifter ska informeras om rätten att när som helst ta tillbaka medgivandet. Förfarandet ska vara enkelt.
* Separata medgivandens ska inhämtas för olika delar av datahanteringsprocessen.
* Barn som är äldre än 13 år kan själv ge sitt medgivande till personuppgiftshantering.
Om barnet är yngre än 13 år krävs vårdnadshavarens medgivande.

3. De registrerades rättigheter utökas
*** Rätt till information**
Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Det är också viktigt att informera om ändamålet med behandlingen. Information om personuppgifts-behandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Om uppgifter kommer att lämnas vidare till andra måste man informera om det.
Individen har rätt att få ta del av de personuppgifter som finns och behandlas i ett register.
Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (kan vara i elektronisk) och med ett tydligt och enkelt språk.
Om det t.ex. skulle inträffa ett dataintrång, identitetsstöld eller bedrägeri måste individen informeras.

*** Rätt till korrigering**
Den enskilde har rätt att begära korrigering av felaktiga eller ofullständiga uppgifter som finns registrerade.

*** Rätt att bli bortglömd**
Varje person har rätt att vända sig till ett företag eller en myndighet som behandlar personuppgifter och be att uppgifterna som avser honom eller henne raderas.
Individen har rätt att få sina uppgifter raderade, men man får inte radera information som lagen kräver att man behåller.
I vissa fall kan individen inte bli bortglömd som t.ex. ett led i myndighetsutövning.

*** Rätt till överflyttning av data (dataportabilitet)**
Individen har rätt att få alla registrerade uppgifter flyttade till en annan organisation.

*** Rätt att göra invändningar**
Individen har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hans eller hennes personuppgifter.
Man är då skyldig att visa att man har behandlat personuppgifterna enligt medgivandet.

*** Rätt till klagomål**
Du kan skicka in tips och klagomål till Integritetsskyddsmyndigheten om du anser att någon bryter mot reglerna för personuppgiftsbehandling.

4. Ha inbyggt integritetsskydd
Det är viktigt att säkra att tjänsterna som används fungerar och att man bara lagrar och hanterar data som är absolut nödvändig. Samla inte på uppgifter som inte behövs.
Spara bara på uppgifter så länge som det är nödvändigt att spara dem. Motivera varför de måste sparas en viss tid.

5. Skyldighet att rapportera incidenter
Om man upptäcker en personuppgiftsincident är man skyldig att rapportera det till Integritetsskyddsmyndigheten inom 72 timmar. Incidenten ska dokumenteras.
En personuppgiftsincident är en händelse som leder till att personuppgifter kommer i orätta händer, förloras eller uppdateras felaktigt.
Den registrerade ska informeras om incidenten om det finns risk för identitetsstöld eller bedrägeri.