



(<http://svenskjazz.se/>)

Information om nya dataskyddslagen GDPR (/sv/för-medlemmar/information-om-nya-dataskyddslagen-gdpr)

Texten uppdaterad senast 2018-05-08

Den 25:e maj 2018 träder den nya dataskyddslagen (GDPR) i kraft och ersätter då fullt ut PUL, personuppgiftslagen.

Den dagen lagen träder i kraft behöver alla föreningar i Sverige ha förberett sig på följande sätt:

- **Gällande medlemskap**

Svensk Jazz har längst ner i vårt ansökningsformulär för nya medlemmar (/sv/f%C3%B6r-medlemmar/bli-medlem) lagt till följande text:

När du trycker på SKICKA godkänner du att Svensk Jazz sparar din information i max ett år efter ett eventuellt utträde ur föreningen, samt via mail gör medlemsutskick med information. Informationen om dig behandlas enbart av administrationen på Svensk Jazz.

Men - när det gäller medlemskap (både framtida och redan befintliga medlemmar) behöver vi antagligen INTE (i alla fall enligt Riksidrottsförbundets vanliga frågor om GDPR (<http://www.rf.se/Personuppgifter/vanligafragor/>)) inhämta samtycke från dessa, eftersom ett ingått medlemskap per definition självklart innebär att uppgifter lämnas och sparas.

Samtycke kan återkallas retroaktivt av medlemmar, som då har rätt att få all sin information raderad. Medlemmen har även **rätt till ett registerutdrag** om vilken information som lagras om den. Förbered så att detta kan åtgärdas om en medlem begär detta.

- **Radera alla inaktiva (över ett år gamla) personuppgifter överallt** - ur medlemsregister och i andra filer i datorn, papper i pärmar etc. Se också över om ni råkar ha irrelevanta uppgifter sparade i registren.

- **Se till att det system som används för att spara och lagra personuppgifter är GDPR-säkert.** När det gäller MyClub, det medlemsregister ni kan använda via ert medlemskap i Svensk Jazz, så tar förbundet ansvar för att sköta den dialogen, som förstås redan är inledd.
- **Skapa en skriftlig policy som kartlägger hanteringen inom föreningen,** där det framgår hur och vem/vilka som hanterar personuppgifter (dvs. den personuppgiftsansvariga samt ev. personuppgiftsbiträden, se förklaring här nedan). Kartlägg i policyn också hur och var ni samlar era register - via ett medlemsregistersystem, i vilka mappar/filer på datorn, i pärmar och/eller i mailkontakter, telefonkontakter etc. Svensk Jazz har nu tagit fram en policy för förbundet. Denna får ni gärna använda som mall för er egen förenings policy. Länk till Svensk Jazz policy (/sv/om-oss/vara-dokument?format=raw&sub_folder=%2Fstyrtdokument&task=download&mime_type=application/pdf&file=Svensk%20Jazz_och_GDPR_p)
- **Glöm inte att även bilder på personer på hemsida och i sociala medier räknas som personuppgifter.**
När det gäller publicering av material på hemsida och sociala medier skriver Riksidrottsförbundet att det "sker det som utgångspunkt med stöd av en intresseavvägning. För det krävs att föreningens intresse av att publicera bilder för att exempelvis visa upp föreningens verksamhet väger tyngre än det intresse personerna på bilderna har av skydd för sina personuppgifter." Det lär alltså alltid vara bäst att fråga de som syns på bilderna innan publicering.
- **Personuppgiftsansvarig** - i en organisation är det alltid styrelse/ledning som ansvarar för registrering av personuppgifter i föreningen. **Personuppgiftsbiträde**, är någon som utanför organisationen delegeras att biträda organisationen på ett sådant sätt att det innefattar att handha personuppgifter. Det kan vara en serverbaserat medlemsregister (som MyClub) eller en redovisningskonsult som skickar fakturor och/eller betalar löner. Organisationen behöver skriva avtal med sina ev. personuppgiftsbiträden. Svensk Jazz återkommer inom kort med ett förslag på hur ett sådant avtal kan se ut.
- **Obehöriga ska ej ha tillgång till medlemsregister och personuppgifter** - Se till att föredetta medlemmar i tex styrelsen till er förening inte fortsätter ha tillgång till personuppgifter efter att de har avgått.

Bra att veta....

- När uppgifter behandlas med stöd av samtycke eller för att uppfylla ett avtal, ska den registrerade ha rätt att få ut de uppgifter man själv lämnat för att föra över dem till en annan tjänst, det kallas **dataportabilitet**.
- Innan man planerar att lägga till fler och andra personuppgifter hos sina medlemmar, som skulle kunna innebära särskilda risker för de registrerade ska man göra en

bedömning av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska riskerna (konsekvensbedömning).

- Om det inträffar en säkerhetsincident, till exempel **ett dataintrång eller en oavsiktlig förlust av uppgifter, måste man anmäla det till Datainspektionen inom 72 timmar**. Man kan också behöva informera de registrerade (anmälan om personuppgiftsincident).
- Vissa organisationer, myndigheter, de som behandlar känsliga uppgifter eller uppgifter som innebär en kartläggning av enskildas beteende måste utse en person i organisationen som har till särskild uppgift att bevaka dataskyddsfrågor, **ett dataskyddsombud**. Men även organisationer som inte måste ha ett dataskyddsombud, kan utse ett ombud.
- Datainspektionen kan komma att **utdöma en sanktionsavgift för den som bryter mot förordningens regler**. Avgiften ska bedömas utifrån hur allvarlig överträdelsen är, om det skett avsiktligt eller inte, vilka åtgärder man har vidtagit för att minska skadan, om man tjänat ekonomiskt på överträdelsen och andra försvårande eller förmildrande omständigheter.
- I personuppgiftslagen finns en förenklad regel för behandling av personuppgifter i löpande text och enkla listor, missbruksregeln. Den innebär kort och gott att man får behandla uppgifter i vissa situationer så länge det inte är kränkande för någon. **Den här regeln försvinner när dataskyddsförordningen träder ikraft**. Sådan behandling måste alltså följa förordningens regler.

Mer ingående information samt checklistor hittar du på www.datainspektionen.se (<http://www.datainspektionen.se>)