Den nya dataskyddslagen och dess konsekvenser

Den 25 maj 2018 träder den nya dataskyddslagen GDPR i kraft. Lagen påverkar hur alla företag och organisationer hanterar personuppgifter, och den kräver en hel del förändringar. Den nya lagen påverkar bland annat hur personuppgifter samlas in, lagras, används, delas och tas bort. Varje steg måste dokumenteras, och varje person har rätt att bestämma exakt hur hans/hennes uppgifter ska hanteras.

Några tips till Kammarmusikförbundets föreningar:

Kartlägg och dokumentera dina data
Du har sannolikt olika personuppgifter på olika ställen, i e-post, i filer, i medlemsregister, i kunddatabaser etc. Du behöver kartlägga och dokumentera hur t ex medlemmars och /eller kunders personuppgifter hanteras. Det innefattar vilken typ av information föreningen har tillgång till, vilka personer och funktioner som har tillgång till den samt i vilka system och databaser den faktiskt finns. Dokumentationen är även viktig om tillsynsmyndigheten skulle genomföra en granskning för att kunna visa på vilka åtgärder ni vidtagit och hur pass väl ni uppfyller kraven. Det gäller att kunna visa att ni aktivt tar ansvar för att följa lagen.

Se över vilka data du har som redan är godkända
Exempelvis data som samlats in för att kunna genomföra en affärstransaktion, eller att personen godkänt exempelvis ett nyhetsbrev. De data som inte är godkända är de som du behöver fokusera på. För att kunna ha en persons uppgifter i ett register kräver den nya lagen ett skriftligt eller muntligt samtycke. Att som person inte protestera när den lagts till i t ex en nyhetsbrevlista dvs.” tyst samtycke” räcker inte.

Kontrollera att du enbart sparar data som du kan försvara
Det gäller att kunna försvara de data som finns i dina register och att du kan berätta vad du behöver dem till. Om ett register innehåller känslig information (sjukdomar, uppgifter om minderåriga, etniskt ursprung etc) så behöver dessa hanteras med särskilt skydd.

Se till att medlemsregistret är uppdaterat enligt nya lagen
Lagen ger en förening rätt att spara en medlem som slutat i 24 månader för att ge föreningen möjlighet att värva den tillbaka. Men efter 24 månader ska den tidigare medlemmen raderas helt ur systemet.

Personers rättigheter
De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med personuppgiftslagen. Länkar till mer information om rättigheterna finns här nedan.

Vad behöver man göra som förening innan 25:e maj?
Som vi tidigare skrivit, så träder den nya lagen GDPR i kraft 25:e maj i år och ersätter då fullt ut PUL, personuppgiftslagen. Den dagen lagen träder i kraft behöver alla föreningar i Sverige ha ordnat följande fem saker:

1. Ordna samtycke från medlemmarna att spara all information som kan knytas till personen. Man måste även kunna styrka att samtycke lämnats.

2. Samtycke kan återkallas retroaktivt av medlem, som då har rätt att få all sin information raderad. Medlemmen har även rätt till ett registerutdrag om vilken information som lagras om personen ifråga.

3. 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 icke relevanta uppgifter sparade i registren.

4. Se till att det system som används för att spara och lagra personuppgifter är GDPR-säkrat.

5. Skapa en skriftlig policy 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 mejlkontakter, telefonkontakter etc.

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 eller en redovisningskonsult som skickar fakturor och/eller betalar löner.
Organisationen behöver skriva avtal med sina ev. personuppgiftsbiträden.

Obehöriga ska inte ha tillgång till medlemsregister och personuppgifter - Se till att före detta medlemmar i t ex 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 innebär 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

Stort tack till Karin Inde på Svensk Jazz, som skrivit den text Kammarmusikförbundet här använder!