Guide för GDPR

ETT PRAKTISKT STÖD FÖR FÖRENINGSLIVET

2024

LEADER 7-sam Värmland

Medfinansieras av Europeiska unionen

SÄFFLE KOMMUN

TORSBY KOMMUN

Munkfors kommun
MUNKFORS | RANSÄTER

Inledning

Det kan vara svårt att förstå vad en som förening behöver göra och hur en ska begränsa sitt arbete i förhållande till GDPR, den EU-förordning som trädde i kraft 25 maj 2018, lagen om personuppgifter, General Data Protection Regulation (GDPR), eller Dataskyddsförordningen på svenska.

Vår rätt till integritet är en mänsklig rättighet. På samma sätt som vi har rätt att låsa vår ytterdörr för tjuvar, har vi rätt till ett privatliv på nätet. Bara vi själva ska bestämma vem vi vill släppa in. Bakgrunden till förordningen det vi kallar GDPR, är helt enkelt att ny teknik har urholkat denna mänskliga rättighet.

När gäller dataskyddsförordningen?

Dataskyddsförordningen gäller för helt eller delvis automatiserad (elektronisk) behandling av personuppgifter. Ett exempel på delvis automatiserad behandling är när personuppgifter samlas in manuellt i syfte att senare föras in i ett automatiserat register. Dataskyddsförordningen gäller också för manuell behandling (pappersform) av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett manuellt register. Vid bedömningen av om det är ett sådant register har det betydelse om informationen är strukturerad så att det enkelt går att hitta information om en enskild person för senare användning.

Det betyder att om ni till exempel har ett register över era medlemmars uppgifter där det exempelvis framgår vad de heter och var de bor så behandlar ni deras personuppgifter och behöver därför följa dataskyddsförordningen.

Vad ni behöver göra

Föreningar behöver följa några grundläggande principer vid behandling av medlemmars personuppgifter.

Bara samla in uppgifter för bestämda och berättigade ändamål d.v.s. Ändamålsbegränsning**:**. Exempel: Om ni har samlat in uppgifter för att administrera medlemskapet ska ni inte senare börja behandla uppgifterna för att profilera medlemmarna för riktad marknadsföring.

Bara samla in uppgifter som är relevanta d.v.s. Uppgiftsminimering**:**
Exempel: Om ni behöver namn och telefonnummer för att administrera medlemskapet ska ni inte registrera personnummer bara för att "det kan vara bra att ha".

Se till att personuppgifterna är riktiga. Riktighet**:**
Exempel: Se till att ha lämpliga rutiner på plats för att säkerställa att felaktiga personuppgifter raderas eller rättas.

Bara spara uppgifter om medlemmar så länge som de behövs d.v.s. Lagringsminimering**:**.
Exempel: Om en medlem avslutar sitt medlemskap ska ni normalt radera eller avidentifiera uppgifterna. Ni behöver ha fastställt hur länge olika uppgifter får sparas och ha rutiner för gallring av personuppgifter.

Skydda personuppgifterna d.v.s. Integritet och konfidentialitet**:** till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs.

Vad är personuppgifter för något?

Personuppgifter är varje upplysning om en identifierbar person. Avgörande är att uppgiften enskilt eller i kombination med andra uppgifter kan knytas till en levande person. Exempel på personuppgifter är:

- namn
- adress och e-postadress
- telefonnummer
- personnummer
- foton.

Vad är behandling av personuppgifter?

Behandling av personuppgifter är allt man kan göra med personuppgifter. Ni behandlar personuppgifter om ni till exempel

- samlar in personuppgifter från medlemmar
- registrerar medlemmar på något sätt
- lagrar personuppgifter någonstans, till exempel i en molntjänst
- lämnar ut uppgifter om en medlem till andra.

ATT GÖRA:

- Ta upp GDPR på nästa styrelsemöte
- Utse en GDPR-ansvarig/dataskyddsombud som ska driva arbetet med att GDPR-säkra föreningen
- Gå igenom och dokumentera hur er förening samlar in och använder personuppgifter
    - Ni bör sträva efter att samla in och behandla så lite information som möjligt så försök att ifrågasätta allt ni samlar in. Detta kallas dataminimering och är en viktig del i GDPR.
    - Detta är den största och viktigaste delen av hela arbetet. Ni säkerställer den personliga integriteten genom att ha koll på vilka personuppgifter ni behandlar och vidtar de åtgärder som krävs utifrån respektive behandling.

- Informera hela er förening, ledare och medlemmar om att ni påbörjat arbetet med att säkerställa efterlevnad av GDPR - Dataskyddsförordningen
- Säkerställ att integritetspolicy och medlemsavtal finns på plats
    - Har ni byggt ert eget medlemsregistersystem så måste ni ta fram en sådan policy och ett sådant avtal. Om ni inte gjort det själva utan köper den tjänsten måste ni se till att de is så fall har en policy och ett sådant avtal på plats.

    - För tips om utformning av integritetspolicy och medlemsavtal, se nedan.

- Se över vilka som har tillgång till era medlemsregister
    - Ett medlemsregister som är tillgängligt för alla medlemmar att se kan vid första anblick vara en bra ide, men det kräver samtidigt att ni berättar för alla era medlemmar att vem som helst i föreningen kan se deras information.

- Utbilda er organisation om det nya regelverket och hur ni kan och ska behandla personuppgifter
- Gå igenom och anpassa avtal och integritetspolicy som rör hantering av personuppgifter
- Utveckla rutiner för hur ni ska göra då ni samarbetar med andra, eftersom varje led i kedjan kan hållas individuellt ansvarigt för hantering av personuppgifter.
- Sedan är det bara att följa era policys, avtal och rutiner. Lycka till!

Att tänka på i arbetet med integrationspolicy

När du skriver en integritetspolicy är det viktigt att den är tydlig, lättförståelig och i enlighet med GDPR. Här är några punkter att tänka på:

1. Tydlighet: Policyn bör vara skriven på ett enkelt och klart språk.
2. Fullständighet: Inkludera all relevant information om hur personuppgifter samlas in, används och skyddas.
3. Laglig grund: Ange den lagliga grunden för behandlingen av personuppgifter. Dvs Dataskyddsförordningen
4. Rättigheter: Förklara de registrerades rättigheter, inklusive tillgång, rättelse och radering.
5. Säkerhet: Beskriv vilka säkerhetsåtgärder som vidtas för att skydda personuppgifter.
6. Kontaktinformation: Ange kontaktuppgifter till den person eller avdelning som ansvarar för dataskydd.

Exempel på medlemsavtal

<u>Personuppgiftsbehandling</u>

Syfte: Förklara varför och hur föreningen kommer att behandla medlemmens personuppgifter.

Samtycke: En klausul där medlemmen ger sitt samtycke till behandlingen av sina personuppgifter.

<u>Medlemmens Rättigheter</u>

Tillgång: Rätten att begära tillgång till sina personuppgifter.

Rättelse: Rätten att få felaktiga personuppgifter rättade.

Radering: Rätten att begära radering av personuppgifter.

Begränsning: Rätten att begära att behandlingen av personuppgifter begränsas.

Dataportabilitet: Rätten att få personuppgifter överförda i ett strukturerat, vanligt använt och maskinläsbart format.

Ansvar och Skyldigheter

Säkerhet: Åtaganden om att skydda personuppgifter mot obehörig åtkomst och förlust.

Dataintrång: Information om förfarandet vid eventuella dataintrång.

Övrigt

Ändringar i avtalet: Hur och när avtalet kan uppdateras.

Tvistlösning: Hur tvister relaterade till avtalet ska hanteras.

Tänk på att detta är ett generellt exempel och att innehållet i ett medlemsavtal kan variera beroende på föreningens specifika behov och verksamhet. Det är rekommenderat att om en har möjlighet konsultera med en juridisk expert för att säkerställa att avtalet är i linje med GDPR och andra relevanta lagar.

LÄNKTIPS

Vad ni som förening behöver göra | IMY