Guide för inventering av personuppgiftshantering NSF

Ett stöd i er anpassning till den nya lagen

Den här guiden är framtagen som ett stöd för er som styrelse/arbetsgrupp när ni inventerar och uppdaterar er hantering av personuppgifter. Det är viktigt för att ni ska följa den nya dataskyddsförordningen (GDPR) som trädde i kraft 25 maj 2018. Det här dokumentet hjälper er genom sex tydliga steg att se över era rutiner.

Den som inte följer förordningen kan i förlängningen få betala stora böter. Skyddet för personuppgifter är inte bara en grundläggande rättighet utan även en fråga om de registrerades förtroende. Förbundet och kårerna har ett gemensamt ansvar för medlemmarnas personuppgifter. Förbundet ansvarar för verksamheten nationellt och medlemsregistrets utformning. Kåren är ansvarig för hur personuppgifterna samlas in och hanteras.

Checklista – så här säkerställer ni att ni följer lagen

1. Ta reda på vad GDPR innebär för er
2. Besluta om **ansvarsfördelning**
3. Gör en **tidsplan**
4. **Inventera** – vilka personuppgifter som hanteras och var de sparas
5. **Rensa** det som inte får finnas kvar och **arkivera** det som ska arkiveras
6. Ta fram **rutiner och riktlinjer** för framtida hantering av personuppgifter
7. **Anpassa verksamheten** till de nya riktlinjerna och håll er uppdaterade

Hjälp om du har frågor

Förbundet lägger löpande upp information och svar på ofta ställda frågor (FAQ) på www.nsf.scout.se/gdpr. Det kommer också att informeras i nyhetsbrev.

Om du har frågor är du välkommen att ställa dem till gdpr@nsf.scout.se eller 08-672 60 80.

Bra information finns också på datainspektionens hemsida www.datainspektionen.se

1. Ta reda på vad GDPR innebär för er

Det är hela styrelsens ansvar att se till att hanteringen av personuppgifter anpassas efter den nya lagen. Förbundet bidrar genom centrala stöd i form av medlemsregister, mallar och riktlinjer som är granskade och godkända enligt den nya lagen.

Det är bra om ni börjar med att diskutera vad ni vet om GDPR och vad det innebär för kåren. Gå igenom materialet som finns på www.nsf.scout.se/gdpr tillsammans. Titta gärna på den webbutbildning som IOGT-NTO har tagit fram. Den kan upplevas lång, men den är grundlig och ni kommer att få en förståelse för vad GDPR är och vad det innebär för er. Information om tillgång till utbildningen finns på www.nsf.scout.se/gdpr

2. Ansvarsfördelning

Styrelsen behöver utse en arbetsgrupp eller person som får till uppgift att leda anpassningen till de nya reglerna. Det bör vara en person som får ansvaret att leda arbetet och se till att ni genomför alla steg i denna guide.

3. Tidsplan

Hjälpdokument: Guide för inventering av personuppgiftshantering NSF

Gör en tidsaxel från nu till den 25 maj och framåt. På den skriver ni när ni ska vara klara med olika delar av arbetet och vem som är ansvarig. Ett förslag på tillvägagångssätt beskrivs i sex steg i detta dokument.

Innan den 25 maj ska ni minst ha genomfört steg 1-3 och ha rensat bort eventuella känsliga personuppgifter som ni inte har rätt att spara. Hinner ni inte genomföra alla steg innan 25 maj ska ni i tidsplanen ha angett hur ni går vidare med att se över era rutiner framöver.

4. Inventering

Hjälpdokument: Inventeringsmall

Skriv ner alla personuppgifter som ni hanterar och var de finns. Till er hjälp finns en inventeringsmall i Excel som NSF tagit fram. I mallen finns kommentarer som vägleder er i ert arbete.

Ett tips är att den utsedda arbetsgruppen börjar att göra inventeringen tillsammans. Därefter kan gruppen avgöra om flera ledare eller andra vuxna i kåren behöver få i uppgift att komplettera er inventering. Inventeringen bör stämmas av i styrelsen eller arbetsgruppen om en sådan utsetts.

Medan ni gör inventeringen är det bra att notera sådant som är bra att systematisera/ändra framöver. Det hjälper er när ni arbetar med att besluta om riktlinjer i steg 5.

Exempel på platser där personuppgifter kan finnas:

- Dokument i datorer
- Bilder, digitala och utskrivna
- Hemsidor
- Fysiska arkiv hemma hos ideella eller i verksamhetslokalen
- Epost till föreningen
- Sociala medier tex Facebook
- Molnbaserade tjänster som Dropbox, Google Drive etc.

Hur kan jag tänka vid en inventering?

I inventeringsmallen finns ett exempel på inventering med kommentarer för att underlätta för er att komma igång.

VAD
- Vilken typ av uppgift är det frågan om?
- Notera om det är en känslig personuppgift eller inte

VARFÖR
- Varför behöver kåren/distriktet ha denna uppgift?
- Vilken laglig grund finns det för att behålla?

VILKEN KATEGORI
- Vilken kategori tillhör ägaren av uppgifterna (medlem, leverantör etc.) I mallen finns ett antal exempel, kanske har ni fler/andra kategorier

NÄR
- När ska uppgiften tas bort? När upphör vårt lagliga behov av den?

VAR
- Var finns uppgiften lagrad?

5. Rensa och arkivera

Hjälpdokument: Rekommendation för rensning och arkivering

När inventeringen av de personuppgifter ni hanterar är gjord är det dags att rensa och arkivera. Till er hjälp i detta arbete finns en rekommendation för rensning och arkivering. Där anges förslag på hur länge det är rimligt att spara olika typer av personuppgifter.

Vad ska jag tänka på när jag rensar?

- Så länge det finns ett berättigat ändamål med att behålla uppgifterna är det ok. Observera att ”Bra att ha” inte är ett tillräckligt argument.

- Tänk på att ni behöver ha en laglig grund och ett ändamål för att behålla och fortsätta behandla det ni har.

Gammalt material behöver bytas ut

Det kommer att krävas ny information och nya former för godkännande/samtycke för hantering av personuppgifter. Förbundet kommer att ta fram texter och mallar att använda

när ni ber medlemmar om godkännande eller samtycke. På grund av detta behöver ni se över och byta ut texter på exempelvis medlemsbekräftelser, anmälningsformulär och bildsamtycke. Gamla broschyrer från förbundet behöver bytas ut då de saknar aktuellt samtycke. Den broschyr som finns i webshoppen (http://www.nsf.scout.se/webshop/) är den aktuella och kan användas.

Vad ska jag tänka på när jag arkiverar?

- Om personuppgifter behöver sparas men kan anonymiseras ska de göra det.
- Arkivering kan göras både fysiskt och digitalt. Oavsett var arkiveringen sker gäller att tillgången till uppgifterna ska vara begränsad och säker. Med begränsad tillkomst menas att endast ett fåtal personer får ha tillgång till arkivet, men fler personer kan få tillfällig tillgång vid behov.

  Observera att allt material inte kan arkiveras. Ni behöver motivera varför det material som arkiveras ska sparas och varför det ska anses vara till allmänhetens nytta.

6. Rutiner och riktlinjer

I steg 3 inventerade ni VAD för uppgifter ni hanterar och VAR de finns. Nu är det dags att arbeta med HUR ni hanterar personuppgifterna. Skapa ett dokument som heter Rutiner och riktlinjer för hantering av personuppgifter. Detta behöver göras tillgängligt för alla som hanterar personuppgifter hos er.

Utgå ifrån er ifyllda inventeringsmall. Gå igenom rutinerna för hur ni hanterar de olika uppgifterna. Dokumentera vilka rutiner ni ska behålla och vilka ni behöver förändra.

När ni gjorde inventeringen i steg 3 uppmanades ni att notera sådant som är bra att systematisera/ändra framöver. De noteringarna ser ni över nu.

Förslag på rutiner att se över:

1. Hur hålls uppgifter uppdaterade? Både i register och på tillexempel hemsidor.
2. Hur säkerställs rutiner för insamling och vidarebefordran av personuppgifter? Behövs biträdesavtal för någon hantering? *Information om biträdesavtal finns på förbundets hemsida.*
3. Hur hanteras känsliga personuppgifter och hur säkerställs att samtycke finns för att lämna dem vidare om det behövs.
4. Ta fram en plan för när uppgifter som samlats in behöver tas bort. Observera att det skiljer sig åt för olika typer av uppgifter. Till er hjälp har ni mallen från förbundet som beskrivs i steg 4.
5. Se över den information som är synlig för medlemmarna. Till exempel på hemsidor, i informationsfoldrar och i verksamhetslokalen.

6. Titta igenom om policys ni har behöver uppdateras. Förbundsstyrelsen fastställer i mars en integritetspolicy för NSF centralt. Den kan ni utgå ifrån och utifrån den se om ni vill göra lokala tillägg.

7. Ta fram en plan för egen incidentrapportering. Mer info om detta kommer att komma från förbundet. Information om detta finns också på datainspektionens hemsida.

8. Se över IT-säkerheten. Behöver ni på något sätt säkerställa högre krav på IT-säkerhet? (Brandvägg, virusskydd, lösenord, lagringsplatser inom/utanför EU)

9. Ta fram en plan för utlämnade av uppgifter om en medlem skulle begära det. Ett centralt registerutdrag för uppgifter som finns i medlemsregistret eBas kan fås via förbundskansliet info@nsf.scout.se

10. Se över hur personuppgifter delas – vilka har tillgång till dem?

7. Anpassa verksamheten

Styrelsen eller ansvarig person bör följa upp att de åtgärder ni kommit fram till vidtas.

Stäm av mot tidslinjen hur ni ligger till.

Ha regelbundna avstämningar även efter den 25 maj så att ni följer de planer ni tagit fram. Gör det gärna till en återkommande punkt på styrelsens dagordning.

Om ni skulle bli utsatta för en kontroll av datainspektionen är det viktigt att kunna visa på vilka åtgärder ni har genomfört och vad er plan är för att säkerställa att ni följer lagen och vilka åtgärder som ni eventuellt har planerat att vidta framöver. Dokumentation av ert arbete är därför viktigt.

Ni kan få en förfrågan från enskilda medlemmar om att de vill få ut alla personuppgifter ni har om dem. Det behöver kunna lösas så snabbt och smidigt som möjligt så prata om hur ni kan möjliggöra det.

Håll er uppdaterade på nyheter och svar på vanliga frågor på www.nsf.scout.se/gdpr och hör av er om ni saknar svar på någon fråga.