STROKE-Riksförbundet

Policydokument. Beslutat 2018-06-08

Innehåll

BEGREPP OCH FÖRKORTNINGAR

Begrepp	Betydelse
Personuppgift	En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Registrerad	Den som en personuppgift avser, det vill säga den fysiska person som direkt eller indirekt kan identifieras genom personuppgifterna.
Personuppgiftsansvarig	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Personuppgiftsbehandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter – oberoende av om de utförs automatiserat eller ej – såsom insamling, registrering, organisering och strukturering.
Personuppgiftsbiträde	En konsult, leverantör eller annan uppdragstagare som utför personuppgiftsbehandling för Riksförbundet eller Förenings räkning.
Personuppgiftsincident	En händelse där obehöriga får tillgång till personuppgifterna eller att personuppgifterna behandlas på ett felaktigt sätt. Händelsen ska innebära fara för registrerades fri- och rättigheter.

1. INLEDNING

I samband med att EU:s dataskyddsförordning (General Data Protection Regulation – GDPR) träder ikraft den 25 maj 2018 behöver personuppgiftsansvariga vidta åtgärder för att anpassa sin personuppgiftsbehandling till den nya lagen. Detta policydokument (härefter**: Policydokument**) innehåller STROKE-Riksförbundets (Härefter**: Riksförbundet**) och de olika länsföreningarnas/lokalföreningarnas (Härefter: **Föreningen** eller **Föreningarna**) organisatoriska åtgärder som ska implementeras i enlighet med GDPR.

Nedanstående åtgärder utgör sådana handlingar och implementeringar som beskrivs i GAP-analysen (12 december 2017), datadelningsavtalet (nr. 0001) och personuppgiftsbiträdesavtalet (nr. 0002). Policydokumentet omfattar all behandling där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data.

Policydokumentet ska börja gälla fr.o.m. 2018-06-08.

2. TILLÄMPNING OCH REVIDERING

Styrelsen hos Riksförbundet ansvarar för att policydokumentet för behandling av personuppgifter upprättas, uppdateras och efterlevs.

Policydokumentet ska revideras och uppdateras av styrelsen hos Riksförbundet minst **en gång per år vid det årliga styrelsemötet** baserat på nya och förändrade regelverk och praxis kring GDPR som berör Riksförbundet eller Föreningarnas organisation. Styrelsen reviderar och uppdaterar policydokumentet tillsammans med länsföreningarna och i tillämpliga fall lokalföreningarna.

Policydokumentet är tillämplig på samtlig personal som verkar inom Riksförbundet, länsföreningarna och lokalföreningarna. Detta innefattar bl.a. styrelseledamöter, medarbetare hos Riksförbundet, länsföreningar och lokalföreningar, konsulter och andra uppdragstagare.

3. ORGANISATION OCH ANSVAR

Styrelsen har det övergripande ansvaret för innehållet i detta policydokument samt att det implementeras och efterlevs av Riksförbundet.

Ordförande för varje enskild förening har det övergripande ansvaret för att innehållet i policydokumentet implementeras och efterlevs av respektive Förening.

Ovanstående ansvariga kan delegera ansvaret och implementationen av detta policydokument till lämplig och behörig person inom respektive organisation.

4. PERSONUPPGIFTSBEHANDLING

4.1 Medlemsuppgifter

Ny medlem

En ny medlem som ansöker om medlemskap ska registreras hos Riksförbundet. Ansvarig person på Riksförbundet ska se till att relevant information (startpaketet) skickas till den nya medlemmen. Medlemskapet utgör en avtalsrelation mellan medlemmen, Riksförbundet och Föreningen.

För Föreningar som har ett avtal om att ha sitt egna medlemsregister med Riksförbundet, ska Riksförbundet, efter att ha mottagit anmälan om medlemskap, skicka över dessa medlemsuppgifter till Föreningen. Därefter ska samtliga medier om personuppgifter (digitala och fysiska kopior) raderas/förstöras/återlämnas.

Evenemang, föreläsningar och andra aktiviteter

Om en Förening vill få ut medlemsuppgifter inför ett event så bör Föreningen maila Riksförbundet om detta. I mailet bör följande uppgifter finnas med:

- Vad det är för typ av event;
- Vilka kategorier av personuppgifter som behövs (t.ex. namn, personnummer etc.);
- Vem som kommer att få ta del av personuppgifterna;
- När personuppgifterna kommer att förstöras/raderas/återlämnas.

Så länge mailet från Föreningen till Riksförbundet om att få ut medlemsuppgifter inte innehåller specifika personuppgifter (t.ex. Kalle Pettersson ÅÅÅÅMMDD-XXXX) kan mailet lagras på obestämd tid. Syftet med ovanstående mailet är att vara ett underlag för om medlemsuppgifterna används på ett godkänt sätt enligt Riksförbundet.

Den ansvarige inom respektive Förening ska se till att endast behöriga personer inom Föreningen får del av personuppgifterna. För att minska riskerna med att personuppgifter kommer i orätta händer bör antalet fysiska kopior begränsas.

Föreningen måste även ansvara för hur många kopior som skrivs ut och som används under eventet. Samtliga kopior måste efter eventet förstöras/raderas/återlämnas. Detta gäller digitala kopior såväl som fysiska kopior.

Medlems rättigheter

Under tiden som medlemmen finns registrerad hos Riksförbundet eller Föreningen har medlemmen rättigheter i enlighet med GDPR. De rättigheter som medlemmar kan komma att begära:

- *Tillgång till personuppgifter:* Medlem som vill få ut sina personuppgifter. Personuppgifterna som finns lagrade hos Riksförbundet eller Föreningen ska kunna fås ut i ett enkelt och läsbart format (t.ex. per mail eller brev).

- *Rättning:* Medlem vill få sina personuppgifter rättade. Om det skulle vara så att namnet, adressen eller någon annan personuppgift inte stämmer, så ska medlemmen kunna få sina uppgifter rättade.

- *Radering:* Medlem vill få sina personuppgifter raderade. Detta är synonymt med att avsluta sitt medlemskap. Riksförbundet eller föreningen får däremot behålla personuppgifter som kan behövas för att uppfylla sina skyldigheter nationell lag (t.ex. bokföringslagen).

Om förfrågan har inkommit till Föreningen så ska Föreningen vända sig till Riksförbundet för att få medlemmens rättighet tillgodosedd. För Föreningar som har sitt egna medlemsregister kan man vända sig till medlemmen direkt. Ovannämnda rättigheter ska kunna utfås så snabbt som möjligt men i alla fall inte senare än **30 dagar** efter att förfrågan inkom.

Riksförbundet eller Föreningen ska innan ovanstående åtgärder utförs, se till att det verkligen är rätt person som begär ut uppgifterna. Detta kan göras genom kontrollfrågor till personen som begär ut uppgifterna eller skicka personuppgifterna till folkbokföringsadressen.

Gallring och radering

När ändamålet med att lagra personuppgifterna har uppnåtts måste personuppgifterna raderas. Nedan ges ett antal exempel på när så kan vara fallet:

- När en medlem avslutar sitt medlemskap;
- När ett event är avslutat och personuppgifterna inte behövs för eventet längre;
- När en forskare inom ett forskningsprojekt som Riksförbundet stödjer inte längre är aktiv inom projektet;
- När en medlem/medarbetare eller annan som har sina personuppgifter hos Riksförbundet återkallar sitt samtycke.

Observera att personuppgifterna kan få behållas under en viss tidsperiod om det behövs i enlighet med nationell lag.

Obehörig person

Medlemsuppgifterna får inte lämnas ut till en utomstående som inte tillhör organisationen. Undantag finns om det förekommer ett avtal med konsult eller uppdragstagare exempelvis.

Personuppgiftsbiträde

Ett företag, konsult, eller annan juridisk person som får ta del av personuppgifterna för Föreningen eller Riksförbundets räkning kallas för personuppgiftsbiträde. Om en sådan ska ta del av personuppgifter måste Föreningen höra av sig till Riksförbundet på förhand för att styrka att detta är **godkänt**. Det måste även finnas ett personuppgiftsbiträdesavtal som stadgar hur personuppgifter kommer att behandlas och när denna kommer att raderas.

Personuppgiftsincident

Inträffar en personuppgiftsincident hos en Förening ska Föreningen genast, och absolut senast **24 timmar**, från att personuppgiftsincidenten inträffade kontakta Riksförbundet för att diskutera vidare åtgärder.

Om personuppgiftsincidenten inträffade hos ett personuppgiftsbiträde ska Föreningen genast, och absolut senast **36 timmar,** från att personuppgiftsincidenten inträffade kontakta Riksförbundet för att diskutera vidare åtgärder.

Om Föreningen tillsammans med Riksförbundet kommer fram till att personuppgiftsincidenten utgör fara för medlemmars fri- och rättigheter (t.ex. fara för bedrägerier, identitetsstölder eller andra fysiska/ekonomiska/sociala konsekvenser) så ska en rapport upprättas och skickas in till **Datainspektionen** (snart namnbyte till Integritetsskyddsmyndigheten). Huvudansvaret för rapporten är Föreningen där personuppgiftsincidenten skedde. Rapporten ska innefatta följande punkter:

- Vad det är som har hänt (datorstöld, hackning, borttappade dokument etc.);
- Vilka personuppgifter det gäller och hur många ungefär som är drabbade;
- Vad personuppgiftsincidenten kommer att leda till;
- Vilka åtgärder som har vidtagits eller kommer att vidtas för att mildra de negativa konsekvenserna (t.ex. låst mobilen för utomstående, spärrat tillgång av personuppgifterna till vidare spridning).

Rapporten måste inkomma till Datainspektionen **senast 72 timmar** efter att personuppgiftsincidenten upptäcktes. Föreningen ska ha kontaktat Riksförbundet inom **24 timmar** (eller om personuppgiftsincidenten skedde hos personuppgiftsbiträdet **36 timmar**) efter att personuppgiftsincidenten upptäcktes.

4.2 E-mail

Hantering av e-mail

När man skickar mail inom organisationen såväl som till utomstående gäller det att vara försiktig. Varje gång personuppgifter skickas över mail ska det ringa en röd varningsklocka. Nedanstående är exempel på vad man bör tänka på:

- Se till att så att det är rätt mottagare till personuppgifterna (speciellt viktigt att tänka på om man har långa förupprättade maillistor);
- Rensa och radera i sin inkorg och utskick efter att personuppgifterna har skickats över;
- Vara extra vaksam över om det är *särskilt känsliga personuppgifter* som man ämnar att skicka. Detta kan vara:
    - Matpreferenser och allergier;
    - Fysiskt- och psykiskt hälsotillstånd;
    - Sexuell läggning;
    - Etnicitet;
    - Etc.[1]
- Undvika att använda sig av öppna nät eller nät som inte är krypterade för obehöriga personer eller andra programvaror som kan komma åt nätet.

4.3 Hemsidan

Korrekta och lagliga personuppgifter

Den ansvarige för hemsidan ska se till att personuppgifter som finns uppe på hemsidan utgör, *korrekta och lagliga* personuppgifter. Att personuppgifterna är korrekta och lagliga innefattar nedanstående exempel:

Samtycke
Personuppgifter som finns uppe på hemsidan (anhörigas berättelser, forskare, bilder på medarbetare etc.) måste ha ett samtycke. Den ansvarige för hemsidan bör försäkra sig om att samtycket finns skriftligt dokumenterat och tillgängligt. Om det inte finns ett samtycke eller om samtycket har återkallats så får informationen inte finnas på sidan.

Uppdatering och radering
Kontrollera att personuppgifterna som finns uppe fortfarande är relevanta. Exempel på när personuppgifterna inte längre är relevanta (läs mer under *Gallring och radering*):

- När en medarbetare har slutat;
- När en medarbetare har ändrat sina kontaktuppgifter;
- När en forskare inte längre är aktiv inom projektet som STROKE-Riksförbund stödjer;

[1] Artikel 9 i GDPR har en uttömmande list över vad som räknas in i *särskilt känsliga personuppgifter.*

- När en person på hemsidan har tagit tillbaka sitt samtycke på att vara publicerad.

Uppdatering och radering bör ske löpande. Dock bör den ansvarige för hemsidan minst **en gång per år** göra en stor inventering av hemsidan och försäkra sig om att alla personuppgifter är relevanta och stämmer.

Driftunderhåll och service

Vid driftunderhåll och service av hemsidan som utförs av en extern konsult bör den ansvarige försäkra sig om att *alla medlemsuppgifter* som finns på hemsidan har överförts till medlemsregistret. Konsulten ska inte kunna komma åt medlemsuppgifterna. Får den externa konsulten tillgång till medlemsuppgifterna kan detta innebära en *personuppgiftsincident* (Läs mer under *Personuppgiftsincident*).

4.4 Facebook

Ordningsregler

För Facebook-sidan som sköts av Riksförbundet bör det finnas ordningsregler och riktlinjer för vad som får göras och sägas i gruppen. Riksförbundet ska vidta åtgärder i förebyggande i syfte och regelbundet hålla uppsikt över vad som publiceras av såväl Riksförbundet som andra medlemmar i gruppen. Nedanstående punkter är särskilt viktiga att tänka på:

- Begränsa behörighet till personer inom Riksförbundet som har administratörsrättigheter till Facebook-sidan;
- Ha ordningsregler som informerar vilka ändamål som kommentarsfunktionen är tänkt att användas och vilka typer av kommentarer eller publiceringar som kan komma att tas bort;
- Ta bort kränkande, hotande eller andra kommentarer som inte har med syftet för gruppen att göra;
- Uppmana användare att rapportera innehåll som kan vara kränkande;
- Ha regelbunden och aktiv uppsikt över vilka kommentarer som skrivs i gruppen.

Uppdatering av information

Minst **en gång per år** uppdatera och se över ordningsreglerna och information som stadgar vilka ändamål som gruppen har.

5. ORGANISATORISKA SÄKERHETSÅTGÄRDER

Både Föreningarna och Riksförbundet måste se till att grundläggande organisatoriska säkerhetsåtgärder finns implementerade hos den egna organisationen. Detta innefattar:

- Att det finns dokumenterat inom Föreningen och Riksförbundet vem som är ansvarig för personuppgiftshanteringen inom respektive organisation;

- Att personal hos Riksförbundet och Föreningarna har relevant och tillräcklig utbildning inom GDPR och IT- och informationssäkerhet för att behandla personuppgifter inom organisationen;
- Att sekretessavtal är tecknat med för samtlig personal hos Riksförbundet, Föreningen eller personuppgiftsbiträdet som hanterar personuppgifter;
- Att det **en gång per år** genomförs kontroller och utvärderingar på att personuppgifter som behandlas inom Riksförbundet/Föreningen fortfarande är nödvändiga och har ett tydligt syfte;
    - Personuppgifter får inte sparas bara för att ”det kan vara bra att ha”, utan då måste personuppgifterna raderas.
    - Om personuppgifterna behövs för ett syfte som är stadgat i nationell lag exempelvis bokföringslagen, bör det frågas om alla personuppgifterna behövs eller om det går att radera delvis av personuppgifterna?
- Att det genomförs kontinuerliga utbildningar och informationsmöten för att försäkra sig om att samtlig personal hos Riksförbundet och Föreningen håller sig uppdaterad;
- Att dokument/listor eller andra fysiska kopior inte finns utspridda på platser där obehöriga personer kan få tag på de fysiska kopiorna;
- Att fysiska kopior av personuppgifter lagras och förvaras i låsta utrymmen när de inte används för tillfället;
- Att digitala kopior av personuppgifter lagras lösenordskyddat och/eller krypterat.

6. TEKNISKA SÄKERHETSÅTGÄRDER

Både Föreningarna och Riksförbundet måste se till att grundläggande tekniska säkerhetsåtgärder finns implementerade på datorn. Detta innefattar bl.a. nedanstående åtgärder:

- Lösenordskyddade datorer;
    - Med både unika användarnamn och regelbundet byte av lösenord.
    - Personnummer, för- och efternamn ska **inte** användas som användarnamn eller lösenord.
- Godkända antivirusprogram och brandväggar;
- Krypterade och lösenordskyddade nätverk där personuppgifter kommer att överföras;
- Använda mailleverantörer som efterlever GDPR;
- Endast utnyttja personuppgiftsbiträden som har hög säkerhetsstandard;
- Undvika öppna nätverk. Nätverk inom Riksförbundet eller Föreningen bör vara lösenord- och krypterat.

Är man osäker på huruvida en viss dator, mobil, surfplatta eller andra medier uppfyller grundläggande krav för säkerhet så bör man dubbelkolla det eller använda sig av andra medier som uppfyller kraven i GDPR. Ovanstående åtgärder är endast ett begränsat urval på säkerhetsåtgärder som bör vidtas.