Policy för trygg hantering av personuppgifter

Inledning

Denna policy har tagits fram för att säkerställa att SeniorNet Sweden och klubbarna i hela nätverket hanterar personuppgifter i enlighet med den nya EU-dataskyddsförordningen 2016/679, nedan kallas GDPR.

Policyn omfattar alla registreringar och behandlingar i SeniorNet Swedens IT-system där personuppgifter hanteras.

Policyn ska fastställas av SeniorNet Swedens styrelse minst en gång per år och uppdateras vid behov.

Bakgrund

Från och med 25 maj 2018 gäller GDPR – General data protection regulation – som slår fast reglerna för behandling av information som kan knytas till en person. Förordningen gäller för myndigheter, företag och organisationer i hela EU och ersätter nuvarande PUL – personuppgiftslagen.

Syftet med den nya lagstiftningen är att få till stånd en harmonisering mellan EU:s medlemsländer samtidigt som fokus ligger på att uppnå ett ökat integritetsskydd för medborgarna. Den enskildes grundläggande rättigheter och friheter stärks, särskilt rätten till skydd av personuppgifter.

Kraven på hur vi som organisation hanterar uppgifter, vilka uppgifter och varför de används är högre än tidigare även om mycket fanns med redan i PUL. Det ska också gå att under vissa omständigheter säga nej till att personuppgifter finns registrerade och används. I det ökade skyddet av individen ingår också rätten att i vissa fall bli borttagen ur register.

Med *personuppgifter* menas varje upplysning som innebär att det går att identifiera en fysisk person; namn, ett identifikationsnummer, en lokaliseringsuppgift, online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig är den juridiska person eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Det innebär att SeniorNet Sweden och också respektive klubb är personuppgiftsansvariga.

Personuppgiftsbiträde är en underleverantör som den personuppgiftsansvarige använder för att hantera personuppgifter. SeniorNet Sweden använder primärt Westarc AB som är leverantör av medlemssystemet arcMember.

Personuppgiftsbiträdesavtal är ett obligatoriskt avtal mellan den personuppgiftsansvarige och biträdet som reglerar vad personuppgiftsbiträdet ska och får göra med personuppgifterna som behandlas för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträdesavtal är under bearbetning och ska tecknas mellan SeniorNet Sweden och Westarc AB.

I bilaga 1 redovisas några ytterligare begrepp i GDPR. I Dataskyddsförordningen definieras begreppen i artikel 3. Begreppen finns redovisade hos Datainspektionen under rubriken Datskyddsförordningen.

Rättslig grund för vår personuppgiftsbehandling

När vi behandlar personuppgifter i vår verksamhet måste vi följa dataskyddsförordningen. Det betyder bland annat att vi ska stödja oss på någon av de rättsliga grunder som finns i förordningen. Utan en rättslig grund är personuppgiftsbehandlingen inte laglig.

Det finns sex rättsliga grunder; samtycke, avtal, intresseavvägning, rättslig förpliktelse, myndighetsutövning och grundläggande intresse. Dessa förklaras närmare av Datainspektionen under rubriken: Rättslig grund för personuppgiftsbehandling.

Vi stödjer oss i huvudsak på den rättsliga grund som innebär att den registrerade/våra medlemmar har ett avtal eller ska ingå ett avtal med vår organisation. Behandlingen är nödvändig för att fullgöra avtalet. Vi måste ha personuppgifter för att exempelvis kunna fakturera medlemsavgiften. Avtalet är lika med våra stadgar som utgör grunden för medlemskapet.

Personuppgiftsbehandling

Personuppgifter registreras och behandlas i vår verksamhet för att administrera medlemskap, hantera deltagande i aktiviteter och för att kunna erbjuda förmåner.

Varje personuppgiftsbehandling ska ske enligt följande principer:

- Vi ska inte behandla fler personuppgifter än nödvändigt (uppgiftsminimering).
- Uppgifterna ska inte ligga kvar längre än nödvändigt och gallras kontinuerligt.
- Samtycke måste inhämtas om det går utanför ramen för avtalet/nödvändiga uppgifter för att verksamheten ska kunna bedrivas.
- Det ska finnas en tydlig beskrivning av ändamålet med att uppgifterna används.
- Den registrerade har rätt till dataportabilitet, vid överflyttning av information till andra system ska rättelse, radering, begränsning av behandling följa med.
- Varje medlem ska kunna ta del av vilka uppgifter som finns registrerade om sig själv
- Eventuella incidenter rörande personuppgifter ska utan dröjsmål rapporteras till SeniorNet Swedens kansli.
- Krav på att personuppgifter hanteras enligt GDPR ska säkerställas vid upphandling och utveckling av IT-lösningar och tjänster.

Förteckning över system i vilka personuppgifter förekommer:
Medlemsregistret ArcMember
Molntjänster
Lokala datorer
Webbplatser (klubbkonceptet och andra webbplatser)
E-post
Externa hårddiskar/arkiv
Anmälningssystem för anmälan till olika aktiviteter
Kassasystem/Ekonomisystem

Kursadministrativa system
Anställningsregistrering i förekommande fall
Lönesystem i förekommande fall

Kategorier av personer:
Medlemmar
Styrelseledamöter
Administrativt behöriga personer
Anställda

Personuppgifter i medlemsregistret arcMember
I enlighet med SeniorNets ändamålsbeskrivning registreras:
För- och efternamn
Födelseår
Medlemsnummer
Adress
E-post
Telefonnummer
Klubbtillhörighet
Eventuell annan information som medlemmen själv uppger vid registreringen angående önskemål om att medverka i det ideella arbetet.

Varje klubbs administrativt behöriga personer har endast tillgång till uppgifter i medlemsregistret som berör den egna lokala verksamheten. Personuppgifter om medlemmar-/besökare/kursdeltagare från andra klubbar hanteras i särskild ordning och vid behov genom SeniorNet Swedens kansli.

SeniorNet Swedens administrativt behöriga personer har tillgång till uppgifter i hela medlemsregistret (för samtliga klubbar).

Personuppgifter används för att kunna:
Fakturera medlemsavgifter.
Fakturera avgifter för kurser, cirklar och övriga aktiviteter som föreningen/respektive klubb tar betalt för.
Göra utskick av information; nyhetsbrev och annan angelägen klubb-/medlemsinformation.
Skicka kallelser till möten.
Skicka inbjudan till kurser och medlemsaktiviteter.
Ta fram nödvändig statistik: antal medlemmar, utveckling över tid, jämförelser mm.
Ta fram underlag för att ansöka om bidrag från studieförbund.
Kontakta personer som vill medverka i föreningens arbete; baseras på medlemmens egna registrerade uppgifter.

Alla utskick till större grupper av medlemmar ska ske via medlemssystemet arcMember; och inte via egna mail-system.

Personuppgifter i medlemssystemet hanteras endast av behöriga administratörer.

Personuppgifterna i medlemssystemet vidarebefordras inte till någon part/annat system utanför föreningens verksamhet om det inte finns ett personuppgiftsbiträdesavtal.

Personuppgiftsansvarig
SeniorNet Sweden är personuppgiftsansvarig och har det övergripande ansvaret för denna policy. Personuppgiftsansvarig är också varje lokal klubb för behandlingen av personuppgifter inom sin verksamhet.

Personuppgiftsbiträdesavtal
SeniorNet Sweden har ett personuppgiftsbiträdesavtal, som revideras löpande, med Westarc AB som är leverantör och sköter driften av vårt medlemssystem arcMember.

Personuppgiftsbiträdesavtal och personuppgiftsunderbiträdesavtal tecknas löpande vid behov. Förteckning över avtal finns på SeniorNet Swedens kansli.

Födelseår
Vid registrering av medlemskap behöver endast födelseår uppges. Tidigare uppgifter om födelsenummer och personnummer är inte nödvändiga uppgifter och är därför borttagna i medlemssystemet.

Medlem kan se vilka uppgifter som finns registrerade
Samtliga uppgifter vi har registrerade om respektive medlem visas efter personlig inloggning i Medlemskort och min profil under fliken Medlem, där medlemmen också själv kan rätta och uppdatera sina uppgifter.

Personuppgifterna raderas när en medlem säger upp sitt medlemskap, eller senast fyra månader efter att medlemskapet har passerat utgångsdatum efter påminnelse. Uppgifterna ska också raderas om en medlem avlider och en anhörig lämnar meddelande om det. Uppgifterna ska gallras kontinuerligt.

Personuppgifter för anställda
Personuppgifter för anställda ska skyddas i enlighet med GDPR. SeniorNet Sweden har ett anställningsavtal med en person vid föreningens kansli. Eventuella anställda vid klubbarna ska ha motsvarande skydd.

Webbplats
SeniorNet Swedens webbplats är försett med SSL-certifikat som säkrar webbplatsen identitet och också att kommunikationen via webbplatsen är krypterad. Det innebär att vid anmälan om medlemskap är kommunikationen krypterad.

Alla klubbar som använder klubbkonceptet har detta certifikat.

För att exponera personuppgifter på webben, exempelvis namn och bild ska vi försäkra oss om att det sker med berörda personers godkännande.

Skydda personuppgifter i digitala arkiv, pärmar och klassiska arkiv
Vi använder antivirusprogram minst det som finns i Windows 10, trådlösa nätverk med kryptering och datorer med uppdaterade program samt lösenordsskydd. Vi säkerhetskopierar även uppgifterna**.**

Det är också viktigt att information som sparas i exempelvis pärmar/arkiv hanteras så att individens integritet skyddas.

Åtgärder ska vidtas för att personuppgifter inte ska vara tillgängliga för obehöriga. Exempelvis bör kontor vara låsta när de är obemannade.

Facebook och andra sociala medier

SeniorNet Sweden har upprättat nya riktlinjer för informationshantering vad gäller Facebook och andra sociala medier.

GDPR – dataskyddsförordningen

EU-Dataskyddsförordningen 2016/679 (GDPR) Källa: Datainspektionen

Tillsynsmyndighet

Datainspektionen är tillsynsmyndighet för GDPR.

SeniorNet Sweden
Byängsgränd 14 3 tr, 120 40 Årsta
E-post: kansli@seniornet.se
Telefon: 08-658 14 60 måndag - onsdag klockan 10-12.
Organisationsnummer: 802403 - 090

Denna policy har inte tagits fram av jurister och kommer att uppdateras löpande.

Bilaga 1: Några begrepp i dataskyddsförordningen.

Bilaga 2: Ny lag i Sverige införs när dataskyddsförordningen börjar gälla.

Bilaga 1

Några begrepp i dataskyddsförordningen.

Ansvarsskyldighet: Dataskyddsförordningen ställer stora krav på dokumentation och att man ska kunna visa att man efterlever lagen.

Behandling: Allting man gör med personuppgifter, till exempel samlar in, registrerar, lagrar, bearbetar eller ändrar, använder, överför eller observerar, är en personuppgiftsbehandling. Det är också oberoende av om det sker automatiserat eller ej.

Intresseavvägning: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Berättigat intresse ska inte misstas för att vara en sorts frihet som ger organisationen möjlighet att fortsätta som tidigare med sin behandling av personuppgifter. En så kallad intresseavvägning måste alltid göras om den rättsliga grunden ska användas.

Dataskydd som standard: Det finns tekniska och organisatoriska krav på att organisationer säkerställer säker hantering av personuppgifter. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

Dataskyddsombud (DPO): Ny befattning med fler formella krav än personuppgiftslagens personuppgiftsombud, förkortas DPO efter engelskans Data Protection Officer. Många, men inte alla, verksamheter är skyldiga att utse dataskyddsombud och anmäla detta till Datainspektionen innan 25 maj 2018.

Incident: Om personuppgifter till exempel kommit på villovägar ska detta anmälas till Datainspektionen inom 72 timmar från det att man fick kännedom om incidenten. Ett gott samarbete med Datainspektionen är viktigt inte minst för att reducera de potentiellt väldigt höga böter som kan utfärdas.

Information: GDPR ställer stora krav på information till den registrerade, bland annat ska information vara lättbegriplig och GDPR definierar i många fall vilken information som måste lämnas i olika situationer.

Rättslig grund: Dataskyddsförordningens artikel 6 listar olika rättliga grunder[1], varav en måste vara uppfylld för att personuppgiftsbehandling ska få göras.

Personuppgift: I princip vad som helst som direkt eller indirekt kan användas för att identifiera en fysisk person. Namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet

Personuppgiftsansvarig: Den juridiska person som ansvarar för personuppgifter.

Personuppgiftsbiträde: Underleverantör som den personuppgiftsansvarige anlitar för att behandla personuppgifter.

[1] Det finns sex rättliga grunder för personuppgiftsbehandling; samtycke, avtal, intresseavvägning, rättslig förpliktelse, myndighetsutövning och uppgift av allmänt intresse eller grundläggande intresse.

Personuppgiftsbiträdesavtal: Ett obligatoriskt avtal mellan den personuppgiftsansvarige och biträdet som reglerar vad personuppgiftsbiträdet ska, och får, göra med personuppgifterna som behandlas för den personuppgiftsansvariges räkning.

Pseudonymisering: En dataskyddsåtgärd som innebär att personuppgifter avidentifieras i den databas de normalt används, men att det finns en nyckel tillgänglig på annat håll. Ska inte förväxlas med kryptering eller anonymisering.

Samtycke: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Samtyckesbegreppet utökas i förhållande till begreppet i personuppgiftslagen. Den som idag har inhämtat samtycke i enlighet med personuppgiftslagen har inte nödvändigtvis längre ett giltigt inhämtat samtycke när GDPR börjar tillämpas. Samtycke är varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Uppgiftsminimering: En central princip i GDPR som handlar om att man inte får samla in fler personuppgifter än vad som är nödvändigt för ändamålet, och inte lagra uppgifter längre än nödvändigt.

Ändamål: Behandling av personuppgifter får endast ske med definierat ändamål, och detta får i princip inte ändras eller utökas i efterhand.

Överföring: GDPR reglerar hur överföring av personuppgifter får ske, i synnerhet om uppgifter lämnas ut till någon, exempelvis ett personuppgiftsbiträde, i ett så kallat tredje land – det vill säga utanför EU. Om Storbritannien inte får till något avtal med EU gällande dataskydd kommer även de att räknas som tredje land efter Brexit.

Dataskyddsförordningen (GDPR) Källa: Datainspektionen
Allmänna bestämmelser

Bilaga 2

Ny lag i Sverige införs när dataskyddsförordningen börjar gälla

Den 25 maj börjar EU:s dataskyddsförordning att gälla, det är en tvingande EU-lag som reglerar hur personuppgifter får behandlas inom EU. I samband med det upphör Personuppgiftslagen (PUL) att gälla och istället införs det en ny lag som kompletterar dataskyddsförordningen.

I den nya lagen, dataskyddslagen, förtydligas det bland annat under vilka förutsättningar vissa personuppgifter får behandlas. Dataskyddslagen tillåter att andra lagar som rör behandling av personuppgifter ändras och uppdateras i samband med införandet av dataskyddsförordningen.

Dataskyddslagen och dataskyddsförordningen får inte tillämpas om de går emot bestämmelserna i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Riksdagen sa ja till regeringens lagförslag. Lagändringarna börjar gälla den 25 maj 2018.

Utskottets förslag till beslut: Bifall till propositionen.
Riksdagens beslut: Kammaren biföll utskottets förslag.

En ny dataskyddslag ska komplettera EU:s dataskyddsförordning: Regeringens pressmeddelande

Ny dataskyddslag: Regeringens beslut.