Reglemente för behandling av personuppgifter och dataskydd

(Tidigare: ”Reglemente för personregister och behandling av personuppgifter inom Medicinska Föreningen”)

Antaget: 2001-09-19

Ändrat: 2010-04-28, 2019-09-26

1 KAP. ALLMÄNNA BESTÄMMELSER

§1 Inledande bestämmelse

Detta reglemente innehåller bestämmelser för hur Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsförordningen, GDPR) och lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning med ändringar och med stöd av dessa utfärdade författningar ska tillämpas inom föreningen.

§2 Ansvarsområde

Styrelsen har övergripande ansvar för behandling av personuppgifter och dataskydd och bistås i detta arbete av datainspektören. Ansvar för att tillämpliga författningar enligt § 1 och att detta reglemente följs åligger dock alla som behandlar personuppgifter inom föreningens verksamhet och använder föreningens data- och IT-resurser. För varje personregister och återkommande och betydande behandlingar av personuppgifter ska det finnas ett ansvarigt kårorgan.

§3 Datainspektör

Styrelsen ska på förslag från Förvaltningsutskottet utse en datainspektör. Uppdraget som datainspektör ska gälla tills vidare. Datainspektören kan när som heslt entledigas av styrelsen.

Datainspektören ska ha till uppgift att

a) övervaka att personuppgifter inom föreningen behandlas korrekt och i enlighet med god sed

b) påpeka eventuella brister i behandlingen av personuppgifter till ansvarigt kårorgan eller styrelsen

c) hålla registret enligt § 4 uppdaterat

d) stödja och hjälpa kårorganen i deras arbete med behandling av personuppgifter så att behandlingen sker lagligt och korrekt och att de registrerades rättigheter uppfylls och att de informeras om dem

e) besluta om beslut måste fattas av styrelsen eller Fullmäktige innan personuppgifter börjar behandlas eller ett personregister inrättas enligt § 14.

f) vid personuppgiftsincidenter leda och samordna styrelsens arbete enligt § 7.

Medicinska Föreningen i Stockholm
Box 250, 171 77 Stockholm
Besök: Nobels väg 10, KI Campus Solna
Tel: 08 – 524 830 71
www.medicinskaforeningen.se

§4 Register över behandlingar

Styrelsen ska se till att det förs ett register över behandlingar av personuppgifter inom föreningen enligt dataskyddsförordningen artikel 30 och att det hålls aktuellt. Registret behöver bara omfatta behandlingar som medför en risk för registrerades rättigheter och friheter, behandlingar som inte är tillfälliga och behandlingar som omfattar känsliga personuppgifter enligt dataskyddsförordningen artikel 9.1 eller artikel 10.

§5 Känsliga personuppgifter

Då känsliga personuppgifter behandlas enligt dataskyddsförordningen artikel 9 ska endast de anställda eller förtroendevalda som behöver ha tillgång till uppgifterna för fullgörande av sina uppdrag ges tillgång till uppgifterna. Personuppgifterna ska skyddas så att andra inte har tillgång till dem.

§6 Skyddade personuppgifter

Person som har meddelat att hen har skyddade personuppgifter, t.ex. hemlig adress, ska få särskild markering i de register där hen förekommer. Uppgifterna får då bara behandlas så att Föreningen uppfyller sina skyldigheter mot personen och inte lämnas ut så att skyddet för uppgifterna äventyras.

§7 Personuppgiftsincidenter

Anställd, förtroendevald eller medlem som får vetskap om en personuppgiftsincident eller en misstänkt sådan ska genast anmäla den till styrelsen och datainspektören. Styrelsen ska se till att vad som har anmälts skyndsamt ska utredas och om det krävs skyndsamt anmäla personuppgiftsincidenten till tillsynsmyndigheten enligt dataskyddsförordningen artikel 33 och informera berörda registrerade enligt dataskyddsförordningen artikel 34. Styrelsen ska se till att alla personuppgiftsincidenter dokumenteras och att korrigerande åtgärder vidtas.

§8 Tekniskt dataskydd

Förvaltningsutskottet och Datornämnden ansvarar för tekniskt dataskydd och säkerhet enligt dataskyddsförordningen artikel 32. De får utfärda föreskrifter inom detta område för att ett fullgott dataskydd ska uppnås.

2 KAP. MEDLEMSREGISTRET

§8 Ansvar och handläggning

För medlemsregistret ansvarar i första led Förvaltningsutskottet. Driften av medlemsregistret sköts av personal på kårexpeditionen och i vissa fall förtroendevalda inom Förvaltningsutskottet.

§9 Innehåll

I medlemsregistret registreras föreningens medlemmar i samtliga medlemskategorier samt studerande vid Karolinska Institutet som enligt stadgarna och högskolelagen har rätt att bli studerandemedlemmar. För varje person kan följande uppgifter anges:

a. namn

b. personnummer

c. adress och postadress

d. telefonnummer och e-postadress

e. uppgifter om adressens riktighet

f. uppgifter om medlemskategori

g. utbildning som undergås vid Karolinska Institutet

h. uppgift om sektionstillhörighet

i. uppgifter från LADOK om registreringar, antagningar och examinationer med relevans för medlemskapet

j. uppgifter om betalningar, skickade räkningar, studentkort o.d.

k. uppgifter om den registrerades *uppdrag* inom Föreningen

l. uppgifter om eventuella fordringar och disciplinära åtgärder mot medlemmar

§10 Utlämnande av uppgifter ur registret

Uppgifter ur medlemsregistret får lämnas ut till följande personer och instanser utanför Medicinska Föreningen endast i dessa fall:

a. den registrerade

b. tryckeri/distributör som anlitas av Föreningen för adressering/tryckning av tidskrift eller annan trycksak som Föreningen ska distribuera till sina medlemmar

c. företag som anlitas som personuppgiftsbiträde för Medicinska Föreningens räkning

d. Karolinska Institutet enligt högskolelagen (1992:1434) 4 kap. 14 § 3 st.

e. företag som anlitas för produktion och distribution av medlemskort och studentrabattkort

f. föreningsmedlemmar genom föreningens matrikel

g. SSCO för SSSB:s verifiering av kårmedlemskap m.a.p. förmånen av studentbostad och kö till sådan.

§11 Undantag för utlämnande till andra

Undantag från bestämmelsen i 10 § kan i enskilt fall beslutas av styrelsen. Sådant beslut gäller maximalt ett år och för det antal utlämningstillfällen som styrelsen beslutar. Vad gäller utlämning av medlemmars adresser för information/inbjudan, ska utlämnandet vägas mot det intresse som medlemmarna har av informationen. Styrelsen kan besluta att debitera en avgift vid utlämnande av registret för riktad information.

Som alternativ till utlämnande av uppgifter ur medlemsregistret för information och inbjudan bör övervägas att utskick i stället sker genom föreningens försorg.

När uppgifter lämnas ut till tredje part ska avtal tecknas om hur länge uppgifterna får användas, hur de ska hållas aktuella och om att de ska destrueras då de inte längre får användas.

§12 Information till de registrerade

Förvaltningsutskottet ska tillse att information lämnas till de registrerade enligt dataskyddsförordningen artikel 12, 13 och 14 samt kommunicera med de registrerade och se till att de registrerades rättigheter enligt artiklarna 15-22 uppfylls. Datainspektören och kårexpeditionen ska vara behjälplig med dessa uppgifter.

3 KAP. ANDRA PERSONREGISTER INOM FÖRENINGEN

§13 Ansvarigt kårorgan

För varje personregister och återkommande eller betydande behandlingar av personuppgifter inom Medicinska Föreningen ska ett ansvarigt kårorgan finnas. Detta organ ansvarar närmast för att lagstiftningen enligt § 1 och detta reglemente följs vad gäller dess personregister och personuppgiftsbehandlingar.

§14 Upprättande av personregister och nya behandlingar av personuppgifter

Innan ett kårorgan behandlar personuppgifter ska datainspektören konsulteras angående behandlingarnas laglighet. Förslag till registerordning enligt § 15 ska inges till datainspektören. Vid tveksamhet kan datainspektören besluta att styrelsen eller – i fall då det gäller styrelsen – Fullmäktige ska besluta om ett personregister får bildas eller om en viss behandling får genomföras.

§15 Registerordning

För varje personregister och återkommande eller betydande behandlingar av personuppgifter ska det ansvariga kårorganet upprätta en registerordning. Av denna ska registrets syfte, funktion, innehåll, mottagare av personuppgifter ur registret, på vilken laglig grund personuppgifterna behandlas, eventuella intresseavvägningar, personuppgifternas lagringstid och om personuppgifter överförs till tredje land framgå.

§16 Personuppgiftsbiträde

Om ett personuppgiftsbiträde anlitas ska alltid ett personuppgiftsbiträdesavtal tecknas. Personuppgiftsbiträdesavtal ska godkännas av styrelsen.

§17 Rapportering av register och behandlingar av personuppgifter

Det åligger det ansvariga kårorganet att till datainspektören rapportera de personregister de har och de behandlingar av personuppgifter som de utför. Dessa förs då in i det register över personregister och behandlingar som denne för enligt § 4. Registerordning som gäller för registret, eventuella personuppgiftbiträdesavtal och information som lämnas till registrerade enligt artikel 13 eller 14 ska också inges till datainspektören. Alla förändringar som görs i hur personuppgifterna behandlas och i registerordningen ska genast rapporteras till datainspektören.

§18 Registerföreskrifter eller -instruktioner

Styrelsen eller – i fall då det gäller Styrelsen – Fullmäktige kan besluta om särskilda föreskrifter (instruktioner då Fullmäktige beslutar) som ska gälla för ett eller flera personregister och behandlingen av personuppgifterna däri.

§19 Information till de registrerade

Det för personregistret ansvariga kårorganet, eller person som detta beslutar, ska tillse att information lämnas till de registrerade enligt dataskyddsförordningen artikel 12, 13 och 14 samt kommunicera med de registrerade och se till att de registrerades rättigheter enligt artiklarna 15-22 uppfylls. Vid svårigheter kan detta hänskjutas till datainspektören. Kårexpeditionen ska vara behjälplig med dessa uppgifter.

Medicinska Föreningen i Stockholm
Box 250, 171 77 Stockholm
Besök: Nobels väg 10, KI Campus Solna
Tel: 08 – 524 830 71
www.medicinskaforeningen.se