Upplýsingaöryggi, varsla gagna og persónuvernd

1. gr. Skjalavarsla og geymslutími gagna

Stjórn félagsins skal tryggja skipulega verndun og vörslu mikilvægra gagna og skjala er varða starfsemi félagsins.

Skalavarsla skal uppfylla skilyrði viðeigandi laga og reglna, m.a. varðandi geymsluform og geymslutíma. Að lágmarki skal geyma eftirtalin gögn samkvæmt neðangreindu:

a. Fundargerðir stjórnar, fastanefnda og annarra mikilvægra starfshópa - óendanlega[1]
b. Undirritaða og endurskoðaða/kannaða ársreikninga félagsins – 25 ár
c. Bókhaldsbækur, bókhaldsgögn og fylgiskjöl – 7 ár frá lokum reikningsárs
d. Formleg samskipti, svo sem í bréfum, tölvupósti o.fl., sem mikilvæg eru í starfsemi félagsins – 7 ár frá lokum reikningsárs
e. Lista yfir þátttöku á viðburðum félagsins vegna staðfestingar á þátttöku og endurmenntunareiningum – 3 ár
f. Að jafnaði skal eyða persónugreinarlegum gögnum þegar þeirra er ekki lengur þörf vegna starfsemi félagsins eða hagsmuna viðkomandi einstaklinga.

2. gr. Skráning persónuupplýsinga

Stilla skal skráningu persónuupplýsinga í hóf, þannig að ekki sé safnað persónuupplýsingum um einstaklinga umfram það sem þörf er á til að tryggja öryggi og hnökralausa þjónustu og rekstur félagsins. Meðhöndlun persónugreinanlegra upplýsinga skal vera í samræmi við ákvæði laga um persónuvernd.

Til að tryggja áreiðanlega auðkenningu félagsmanna og þátttakenda í viðburðum félagsins og auðvelda samskipti heldur félagið utanum skráningar, sem innihaldið geta m.a. upplýsingar um nafn, heimilisfang, tölvupóstfang, símanúmer, meðlimanúmer hjá alþjóðasamtökum innri endurskoðenda (IIA) og kennitölu viðkomandi einstaklings, prófgráður eða fagvottun sem máli skipta í tengslum við starfsemi félagsins og upplýsingar um vinnustað viðkomandi, starfsheiti og fleira slíkt. Í meginatriðum er um að ræða:

a. Félagatal, sem er grundvöllur að innheimtu félagsgjalda, veitingu afsláttar af þátttökugjaldi viðburða og öðrum samskiptum við félagsmenn.
b. Póstlistar, sem ýmist eru byggðir á félagatali, frjálsri skráningu á póstlista óháð því hvort viðkomandi er félagsmaður, þátttökulistum vegna tiltekinna viðburða eða öðrum listum sem sérstaklega eru útbúnir í tengslum við tiltekna viðburði eða verkefni.
c. Grunnskráningu félagsmanna hjá alþjóðasamtökum innri endurskoðenda (IIA), sem er grundvöllur fyrir ýmissi þjónustu sem aðgengileg er félagsmönnum aðildarfélaga og þjónustu sem samtökin sjá um fyrir hönd félagsins gagnvart félagsmönnum þess.
d. Þátttökulistar atburða vegna innheimtu þátttökugjalda og staðfestingar á þátttöku, m.a. ef einstaklingur þarf síðar staðfestingu á mætingu vegna endurmenntunareininga tengdum fagvottunum, viðhaldi löggildingar o.s.frv.

[1] Óendanlegur geymslutími er notaður þar sem gögn gætu verið mikilsverðar heimildir um sögu og starfsemi félagsins.

Félag um innri endurskoðun

3. gr. Notkun skráðra persónuupplýsinga

Óheimilt er að afhenda, hvort sem er gegn gjaldi eður ei, skráðar persónuupplýsingar um félagsmenn nema að undangengnu samþykki þeirra. Beiðni um slíkt samþykki skal tilgreina til hvaða nota félagið hyggst afhenda upplýsingarnar.

Ákvæði 1. mgr. þessarar greinar gilda m.a. um dreifingu félagatals og póstlista, en við útsendingu tölvupósts skal gætt að því að póstlistar séu ekki aðgengilegir móttakendum til frekari notkunar.

4. gr. Öryggi gagna og upplýsingakerfa

Gætt skal að því að öll gögn og upplýsingar félagsins séu varðveittar á tryggan hátt og komið í veg fyrir með hæfilegum og viðeigandi aðgerðum að óviðkomandi komist í gögnin. Til þess skal að lágmarki beitt eftirfarandi aðgerðum í allri starfsemi félagsins:

a. Gögnum sem varðveitt eru á pappírsformi sé safnað saman og komið í trygga geymslu, þau vistuð í tilskilinn tíma skv. 1. gr. þessara reglna og eyðing í lok geymslutíma fari fram á viðurkenndan og öruggan hátt.
b. Hæfilegar og viðeigandi ráðstafanir séu ávallt gerðar til að verja samskipti við vefsíður félagsins.
c. Notendanöfn og lykilorð séu varin með fullnægjandi hætti og þess gætt að lykilorð séu hvergi sýnileg.
d. Viðkvæmum aðgangi sé úthlutað og hann afturkallaður eftir því sem breytingar verða á stjórn og nefndum og hlutverki einstakra aðila.
e. Aðgangur sé opnaður að vefsvæðum sem eru lokuð öðrum en félagsmönnum þegar einstaklingur gengur í félagið og honum lokað þegar viðkomandi hættir.
f. Reglulega sé farið yfir aðgangsheimildir að vefsíðum og öðrum kerfum sem félagið notar í starfsemi sinni.
g. Gætt sé að því að mikilvægar hugbúnaðaruppfærslur séu ávallt gerðar án tafar, sérstaklega þær sem varða öryggi vefsíðna og gagnasafna sem félagið nýtir í starfsemi sinni.

Í þeim tilfellum sem félagið nýtir aðkeypta þjónustu í störfum sínum skal stjórn ganga úr skugga um að viðeigandi varúðarráðstafanir séu til staðar hjá þjónustuaðila í samræmi við reglur þessar og almennar kröfur til slíkra aðila. Jafnframt skal gætt að því að viðeigandi gögn skili sér frá slíkum aðilum til félagsins til vörslu í samræmi við reglur þessar.

5. gr. Ábyrgð og eftirfylgni

Formönnum fastanefnda, faghópa og annarra starfshópa á vegum félagsins ber að tryggja að verkefni sem viðkomandi nefndir og hópar bera ábyrgð á séu unnin í samræmi við reglur þessar.

Stjórn skal fylgja því eftir að reglum þessum sé fylgt í allri starfsemi félagsins og tryggja að mikilvægum gögnum frá undirnefndum og starfshópum sé skilað til stjórnar til vörslu í samræmi við reglurnar.

Til breytinga á reglum þessum þarf einfaldan meirihluta stjórnarmanna.

Samþykkt á stjórnarfundi 18. maí. 2017