CHECKLISTA FÖR STYRELSEN I EN BOSTADSRÄTTSFÖRENING

Nedan är förslag på åtgärder som styrelsen i en bostadsrättsförening kan börja arbeta med för att följa de krav som ställs enligt GDPR.

1. INVENTERA OCH GÖR ETT ENKELT REGISTER

Enligt GDPR behöver den som är personuppgiftsansvarig (bostadsrättsföreningen) ha kännedom om de personuppgifter som föreningen hanterar. Ett bra första steg är därför att inventera vilka personuppgifter bostadsrättsföreningen hanterar idag och vart de förekommer.

Vidare ställer GDPR krav på att personuppgiftsansvariga ska föra ett register över sina personuppgiftsbehandlingar. Registret ska inte vara en fullständig lista över alla personuppgifter i detalj som föreningen hanterar för enskilda personer. Registret ska framförallt lista kategorier av enskilda vars personuppgifter föreningen hanterar (till exempel medlemmar, hyresgäster och anställda) samt kategorier av personuppgifter som hanteras (till exempel adresser och betalningshistorik).

Att göra:

✔ Börja med att göra en grov inventering av *vilka personuppgifter* föreningen hanterar och *vart de förekommer* för att få en första uppfattning av omfattningen av personuppgifter och vart de finns. Inventeringen kan förslagsvis läggas upp med stöd av följande frågor:

- Vilka kategorier av enskilda personer (bostadsrättsinnehavare/medlemmar, hyresgäster, anställda, styrelseledamöter) finns det information om?
- Vilken typ av personuppgifter rör det sig om?
- Vad används informationen till?
- I vilka system (mailkonto, webbplats, mappar på datorn, olika IT-tjänster, molntjänster, etc.) och på vilka fysiska platser (fysiska pärmar, arkiv, etc.) förekommer informationen?
- Vilka har tillgång till informationen? Lämnas informationen ut till någon?

✔ Gör därefter/samtidigt ett enkelt register över bostadsrättsföreningens personuppgiftshanteringar. HSB har tagit fram en mall för detta.

2. HAR VI RÄTT ATT SPARA PERSONUPPGIFTEN?

Bostadsrättsföreningen bör även se över om föreningen har rätt att spara de personuppgifter som föreningen i dagsläget hanterar. Grundläggande krav enligt GDPR är nämligen att det ska finnas ett relevant ändamål till varför personuppgiften sparas.

Dessutom måste bostadsrättsföreningen ha stöd i någon av de sex lagliga grunder som finns i GDPR för att få hantera personuppgiften. De grunder som framförallt kan vara aktuella är att personuppgiften behövs för att fullgöra ett avtal med den enskilde eller för att fullgöra en rättslig förpliktelse eller att den enskilde har lämnat sitt samtycke till den aktuella behandlingen. Läs mer om de lagliga grunder som framförallt är aktuella för bostadsrättsföreningar på sidan 12.

Att göra:

✔ Bostadsrättsföreningen bör se över vilken laglig grund som finns för föreningens hantering av personuppgifterna.

✔ Bostadsrättsföreningen bör även fundera igenom vad ändamålet med att spara uppgiften är, det vill säga vad ska uppgiften användas till? Behövs den verkligen för det användningsändamålet eller räcker det med mindre omfattande information? Läs mer om så kallad ”ändamålsbegränsning” och ”uppgiftsminimering” på sidan 13.

3. GALLRA

Eftersom bostadsrättsföreningen endast får spara personuppgifter om det finns en laglig grund och ett berättigat ändamål (som fortfarande är aktuellt), ställs numera högre krav på föreningens gallringsrutiner.

Att göra:

- ✔ Börja med att se över och rensa bort gammalt material där det finns personuppgifter som inte längre behövs. Tänket ”bra att ha” håller inte längre. Om det inte finns laglig grund och/eller ett verkligt behov ska personuppgiften inte sparas.
- ✔ Inför gallringsrutiner enligt vilka en regelbunden kontroll görs av de personuppgiftsbehandlingar bostadsrättsföreningen gör.

4. PERSONUPPGIFTSBITRÄDESAVTAL

Enligt GDPR måste det finnas ett personuppgiftsbiträdesavtal med alla företag som behandlar personuppgifter för föreningens räkning, till exempel förvaltningsbolag och entreprenörer.

Att göra:

- ✔ Säkerställ att bostadsrättsföreningen har ingått personuppgiftsbiträdesavtal med alla leverantörer som hanterar personuppgifter för föreningens räkning.

5. SE ÖVER BEHÖRIGHET OCH TILLGÅNG TILL INFORMATION

Med anledning av de höga krav som GDPR ställer på säkerhet av hantering av personuppgifter bör bostadsrättsföreningen se över behörighet och tillgång till information i föreningen.

Att göra:

- ✔ Se över och – om nödvändigt – begränsa vilka som har behörighet till bostadsrättsföreningens mailkonton, IT-system och andra inloggade gränssnitt där det finns personuppgifter. Endast de som behöver informationen i sitt uppdrag ska ha tillgång till den.
- ✔ Se även över eventuellt pappersarkiv eller liknande där det finns personuppgifter och säkerställ att det är inlåst på ett betryggande sätt och bara kan tillgås av de som behöver informationen i sitt uppdrag.

6. SE ÖVER DIGITALA KANALER

Det kan vara lätt att glömma att personuppgifter även kan finnas i bostadsrättsföreningens digitala kanaler, tillförda av föreningen eller av annan, varför dessa bör ses över.

Att göra:

- ✔ Om föreningen har en egen webbplats och/eller konto på sociala medier där det förekommer personuppgifter bör det ses över om dessa behöver gallras och/eller uppdateras.
- ✔ Vanligt är att man glömmer att webbplatsen kan innehålla så kallade fritextfält exempelvis vid kontaktformulär. Det bör i så fall övervägas om dessa kan tas bort eller om det bör föras in information om att personuppgifter inte ska skrivas in i fritextfälten.

7. UPPRÄTTA RUTINER

Med tydliga nedskrivna rutiner blir det enklare både för befintliga och nya styrelseledamöter att göra rätt. Det är även viktigt att ha dokumenterade åtgärder så att bostadsrättsföreningen kan visa att kraven i GDPR efterlevs.

Att göra:

- ✔ Sätt upp en enkel rutin för hantering av personuppgifter i era olika system samt eventuell pappershantering – från insamling av personuppgiften till gallring av densamma! HSB kommer att tillhandahålla en personuppgiftspolicy för bostadsrättsföreningar inom kort.

8. LÄGG EN PLAN FÖR DET FORTSATTA ARBETET

Många organisationer kommer att ha problem med att fullt ut följa GDPR till den 25 maj 2018. Det är dock viktigt att ni i vart fall påbörjar arbetet omgående och att ni lägger upp en tydlig plan för hur arbetet ska utföras framåt.