FRÅGOR OCH SVAR

Hur påverkar GDPR bostadsrättsföreningen egentligen?

GDPR påverkar alla stora och små organisationer (däribland bostadsrättsföreningar). Det krävs nya rutiner för hantering av personuppgifter som måste genomsyra hela verksamheten.

Gäller GDPR både för personuppgifter som föreningen sparat i elektronisk och fysisk form?

GDPR gäller för all elektronisk hantering av personuppgifter. GDPR gäller även för annan hantering än elektronisk (till exempel nedskrivning av personuppgifter i minnesanteckningar eller andra handskrivna papper som innehåller personuppgifter) om de ingår i ett register. De fysiska papperna ska alltså vara strukturerade och sökbara i någon form av register (till exempel indexerade pärmar/katalogiserade arkiv). Även om GDPR inte gäller för en enskild fysisk handling är det såklart viktigt att föreningen har en säker hantering även av sådana handlingar.

Måste föreningen ha ett register över sina personuppgiftsbehandlingar? Hur gör man i sådana fall ett sådant register?

Ja, med anledning av den mängd personuppgifter som bostadsrättsföreningen behandlar om exempelvis sina medlemmar och styrelseledamöter, kommer bostadsrättsföreningen behöva upprätta och förvalta ett register över sina personuppgiftsbehandlingar. I GDPR finns specifik information om vad ett sådant register ska innehålla. Primärt ska ett register innehålla; i) kontaktuppgifter till föreningen, ii) ändamål med behandlingen, iii) en beskrivning av kategorier av registrerade, iv) kategorier av personuppgifter och v) kategorier av mottagare till vilka personuppgifter lämnas ut till.

Det finns flera systemstöd för register på marknaden. Om mängden behandlingar inte är så omfattande går det bra att till exempel skapa ett register i Excel eller Word. HSB tillhandahåller en sådan mall.

Vilket ansvar har styrelsen för att bostadsrättsföreningen följer GDPR?

Styrelsen ansvarar för föreningens organisation och förvaltning. Styrelsen har även en vårdplikt som innebär att styrelsen ska se till föreningens intressen och bästa. Det ligger i föreningens intresse att följa GDPR bland annat eftersom en god regelefterlevnad minskar risk för att föreningen får betala sanktionsavgifter (till staten) och/eller skadestånd (till enskilda) som kan bli följden vid bristande regelefterlevnad. Det är även i föreningens intresse att ha god ordning och reda. Ett tips är att eventuellt utse en ledamot i styrelsen som ska ha särskilt ansvar för dessa frågor.

En medlem har begärt att få ut de personuppgifter som föreningen har sparat avseende denne, vad gäller?

Medlemmen har rätt att ta del av de personuppgifter som föreningen behandlar om medlemmen. Utlämnandet av informationen underlättas av om föreningen har ett register över sin personuppgiftsbehandling.

Vilka måste föreningen ha personuppgifts-biträdesavtal med?

Föreningen måste ha personuppgiftsbiträdesavtal med alla aktörer som behandlar personuppgifter för föreningens räkning, till exempel förvaltare och leverantör av passerkortsystem.

Vilka personuppgifter får föreningen skriva in i lägenhetsförteckningen?

Föreningen ska ha en laglig grund och ett berättigat ändamål för att få behandla personuppgifter. Det finns obligatoriska krav på vilka uppgifter (här innefattas också personuppgifter) som ska framgå av lägenhetsförteckningen i bostadsrättslagen. Föreningen har därmed en laglig grund (se den lagliga grunden ”rättslig förpliktelse” på sidan 12) för att få registrera dessa uppgifter.

Det är dock vanligt att föreningar antecknar uppgifter utöver vad som framgår av lagen i lägenhetsförteckningen, exempelvis om överlåtelser, vilket kan vara praktiskt. Det går att göra så länge det finns en laglig grund och ett rimligt ändamål. När uppgifterna inte längre behövs måste de raderas. Det rekommenderas dock att så lite uppgifter som möjligt förs in i förteckningen och endast sådant som föreningen behöver för sin verksamhet.

Vilka uppgifter får föreningen skriva in i medlemsförteckningen?

Föreningen ska ha en laglig grund och ett berättigat ändamål för att få behandla personuppgifter. Det finns obligatoriska krav på vilka uppgifter (här innefattas också personuppgifter) som ska framgå av medlemsförteckningen i bostadsrättslagen. Föreningen har därmed en laglig grund (se den lagliga grunden ”rättslig förpliktelse” nedan) för att få registrera dessa uppgifter.

Då medlemsförteckningen – till skillnad från lägenhetsförteckningen – ska vara tillgänglig för den som vill ta del av den rekommenderas det att det inte skrivs in några personuppgifter i denna utöver vad lagen anger, det vill säga uppgift om medlemmens namn och postadress samt om den bostadsrätt som medlemmen har.

Gäller GDPR för föreningens passerkortsystem (dvs. elektronisk passage)?

Ja. Det är vanligt att passerkort är knutna till en enskild person och dess lägenhetsnummer som antecknas i ett register. Vidare är det vanligt att loggar kan tas fram för när och vart passage har skett för de enskilda passerkortsinnehavarna. GDPR gäller för dessa register och loggar. Det är viktigt att föreningen förvarar denna information säkert och att endast de som behöver informationen har tillgång till den (vanligtvis behöver inte styrelseledamöter tillgång till denna information). Ändamålet med passerkortssystemet är rimligen att kunna låsa och upprätthålla säkerheten i föreningens fastighet. Personuppgifterna (loggarna) får endast användas i detta syfte och på ett sätt som de enskilda fått information om. Personuppgiftsbiträdesavtal måste ingås med leverantören av passerkortssystemet.

Gäller GDPR om en styrelseledamot administrerar föreningens ärenden hemma på sin egen dator istället för på en dator ägd av föreningen?

Ja. GDPR gäller inte för privatpersoners hantering av personuppgifter, det vill säga sådant som ligger utanför yrkes- eller affärsverksamhet. En styrelseledamots administration av föreningens ärenden utgör dock inte privat hantering av personuppgifter – GDPR gäller därför fullt ut. Det spelar ingen roll om datorn som styrelseledamoten använder är privat eller om arbetet sker hemma och inte i föreningens lokaler.

Kan föreningen fortsätta att använda molntjänster (dvs. IT-tjänster som tillhandahålls över internet, till exempel Dropbox och Google Drive) för att spara elektronisk dokumentation (som kan innehålla personuppgifter)?

Ja, men endast om föreningen tillförsäkrar sig om att god säkerhet uppnås. GDPR ställer höga krav på att information sparas på ett säkert sätt och att den inte kan nås av obehöriga. Det rekommenderas därför att föreningen endast använder företagsversioner av dessa tjänster och inte styrelsemedlemmars privata versioner. Föreningen bör även se över så att endast de som behöver informationen i molntjänsten har tillgång till den. Personuppgiftsbiträdesavtal måste ingås med leverantören av molntjänsten.

Vad finns det för risker om föreningen inte följer GDPR?

De största riskerna om föreningen inte följer GDPR är att föreningen kan drabbas av sanktionsavgifter som kan uppgå till betydande belopp, beroende på överträdelsens allvarlighetsgrad och andra försvårande eller förmildrande omständigheter. Vidare kan föreningen även få betala skadestånd till eventuell enskild som drabbats av överträdelsen.