

GDPR.

Vägledning för
bostadsrättsföreningar

**För att få hantera
personuppgifter
måste föreningen
ha en laglig
grund för detta.**



En skillnad mellan GDPR och PUL är att enligt GDPR får ni endast hantera de personuppgifter ni har laglig rätt att hantera eller har inhämtat samtycke till.

INLEDNING

INFORMATION

Dom som sitter i styrelsen behöver ha information om vad GDPR innebär och vad som kommer att gälla. Även om föreningen inte hanterat registren själv utan har ett eller flera personuppgiftsbiträden (tex ekonomisk förvaltare) behöver ni vara medveten om vikten av att handskas försiktigt med personuppgifter.

Troligtvis har föreningen medlemslistor i andra former för att exempelvis nå ut med information till medlemmarna. Eller kontaktlistor för personer hos lokalhyresgäster, anställda hos förvaltare, byggbolag, leverantörer och samarbetspartners.

1 VILKA PERSONUPPGIFTER HAR NI?

Vilka register har vi? Vilka personuppgifter hanterar vi i registren, varifrån får vi dem och vem lämnar vi ut dem till? Har vi fler uppgifter i registren än som behövs för ändamålet? Hur ofta uppdateras de, och raderas inaktuella register?

Att göra:

- ✓ Utse eventuellt en personuppgiftsansvarig i styrelsen och skapa en rutin för hur ni hanterar personuppgifter (om ni inte redan har det).
- ✓ Skapa en registerförteckning över vilka register ni har i bostadsrättsföreningen

Exempel: är medlemsregister, lägenhetsförteckning, kontaktlistor, hyresgästlistor, nyckellistor, hemsidor, mail etc.

2 FÖR ETT REGISTER ÖVER FÖRENINGENS PERSONUPPGIFTER

Som bostadsrättsförening får ni enbart behandla personuppgifter i den omfattningen som behövs för att fullgöra ändamålet med behandlingen: till exempel att tillhandahålla bostäder, p-platser eller lokaler och kunna kommunicera samt skicka ut avier för avgifter och hyror.

Att göra:

- ✓ Upprätta register över vilka behandlingar ni genomför.
- ✓ Gå igenom vem ni lämnar ut registerna med personuppgifter till.
- ✓ Gå igenom så att ni inte lämnar ut personuppgifter till annan part utan att denne lämnat samtycke till detta.
- ✓ Gå igenom vilka leverantörer ni har som hanterar personuppgifter åt er.

3 SÄKERSTÄLLA ATT FÖRENINGEN HAR RÄTT ATT HANTERA PERSONUPPGIFTERNA

Som bostadsrättsförening får ni enbart behandla personuppgifter i den omfattningen som behövs för att fullgöra ändamålet med behandlingen: till exempel att tillhandahålla bostäder, p-platser eller lokaler och kunna kommunicera samt skicka ut avier för avgifter och hyror.

Vad gäller medlemsförteckning och lägenhetsregister så finns det stöd för den hantering i lagen om ekonomiska föreningar och Bostadsrättslagen. En annan laglig grund för hantering av personuppgifter är att det nödvändigt för att fullgöra ett avtal, i föreningens fall är ett bra exempel på detta ett hyresavtal. I övriga fall krävs samtycke, tex för publiceringar på föreningens webb.

I GDPR är att missbruksregeln är borttagen. Det innebär att även personuppgifter i ostrukturerad form berörs av GDPR. Det innebär att personuppgifter i pärmar, papper, mail etc numera ingår

Att göra:

- ✓ Gå igenom inventeringen och säkerställ att det finns laglig grund för respektive personuppgift ni registrerar.
- Utnyttjar föreningen missbruksregeln i dag? Exempelvis när det gäller publicering av namn, e-postadresser, bilder eller videor på föreningens webbplats eller i e-postprogram? Har medlemmarna i så fall informerats på rätt sätt och gett sitt medgivande? Föreningen måste kunna visa att ett samtycke har lämnats.

4 GÖR EN ÅTGÄRDSPLAN FÖR HUR FÖRENINGEN SKA EFTERLEVA KRAVEN PÅ BEHANDLING AV PERSONUPPGIFTER

GDPR ställer ett antal krav på hantering och behandlingen av personuppgifter. Det ska finnas tekniskt skydd (säkerhet) och ett fastställt arbetssätt så minimera risken att personuppgifterna sprids obehörigen. Behandlingen får endast ske för det eller de ändamål som personuppgifterna samlats in för. Personuppgifterna får inte användas eller lagras under längre tid än vad som krävs för att uppfylla ändamålen samt att föreningen kan rätta och ta bort felaktiga uppgifter.

Att göra:

Ta fram en rutin för hur personuppgifterna ska hanteras.

En rutin som bland annat innefattar: Vilka och hur personuppgifter samlas in, var och hur de används.

Hur personuppgifterna ska kontrolleras och uppdateras.

- ✓ Vilka uppgifter som ska gallras (raderas) och när de i sådana fall ska gallras. Hur personuppgifterna ska förvaras och med vilken säkerhet som de hanteras (gäller såväl teknisk som vilka personer som ska ha rätt att få tillgång till personuppgifterna).
- ✓ Upprätta en åtgärdsplan utifrån den fastlagda rutin för att dokumentera och säkerställa att föreningen efterlever GDPR.



Ta fram en tydlig policy för personuppgifter så att det är enkelt om/när styrelseledamöter byts ut att fortsätta följa GDPR-regelverket.

GDPR

UPPRÄTTA AVTAL MED PERSONUPPGIFTSBITRÄDEN

Ett personuppgiftsbiträde får endast behandla personuppgifter i enlighet med föreningens (personuppgiftsansvariges) instruktioner.

Att göra:

- ✓ Se till att få skriftliga personuppgiftsbiträdesavtal upprättade och undertecknade.
- ✓ Att biträdes avtalet är kopplat till ett huvudavtal

BEGREPP

PERSONUPPGIFTER: All slags information som antingen direkt eller indirekt (det vill säga via annan information) kan kopplas till en fysisk person, exempelvis namn, personnummer, e-postadress, lägenhetsnummer, fotografier eller film- och ljudfiler.

BEHANDLING: Åtgärd eller kombination av åtgärder med personuppgifter oberoende om de utförs automatiserat eller inte.

PERSONUPPGIFTSANSVARIG: Den som bestämmer ändamål och medel för personuppgiftsbehandlingen och därmed är ansvarig för att den sker i enlighet med gällande lagar, i detta fall bostadsrättsföreningen.

PERSONUPPGIFTSBITRÄDE: Det företag eller den organisation som behandlar personuppgifter på uppdrag av personuppgiftsansvarig - föreningen - för dennes räkning, exempelvis en ekonomisk förvaltare.

KONTAKT

Behöver ni hjälp med att upprätta Policy, behandlingsregister m.m. kontakta

Namn

Telefon

E-post

Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade



General
Data
Protection
Regulation