STEP LOCK ACCESS

Gäller GDPR för min BRF?

Informationsbroschyr om GDPR riktat till BRF.

Beskrivning

Från och med den 25 Maj 2018 trädde GDPR i kraft. GDPR är den nya dataskyddsförordningen som efter 20 år tar över efter PUL.
GDPR (General Data Protection Regulation) slår fast reglerna för all form av behandling av information som direkt eller indirekt kan knytas till en person.

Syftet med den nya lagstiftningen är bl.a. att få till en harmonisering av tillämpningen av det tidigare dataskyddsdirektivet mellan EU:s medlemsstater. Dataskyddsdirektivet från 1995 utgjorde visserligen en gemensam grund inom unionen, men som direktiv var det upp till varje land att implementera regelverket och tolka det. Nu är det samma lagtext oavsett vilket EU-land man befinner sig i.

Samtidigt har det legat mycket fokus på ett ökat integritetsskydd och ytterligare ett syfte med GDPR är att stärka EU-medborgares rättigheter i förhållande till sina personuppgifter.

GDPR är en lag som alla företag, myndigheter och organisationer, även bostadsrättsföreningar, måste känna till och följa.

GDPR har ersatt PUL

Dataskyddsförordningen, GDPR*, ersatte den 25 maj 2018 den tidigare personuppgiftslagen, PUL, från 1998. Den ersatte också EU:s dataskyddsdirektiv från 1995.

Mycket av det som GDPR reglerar har gällt sedan 1998, i och med PUL, men en del regler har blivit strängare. När dataskyddsförordningen ersätte personuppgiftslagen blev den så kallade missbruksregeln inte längre kvar. Missbruksregeln innebär att enklare regler gäller för personuppgifter i ostrukturerat material. Det handlar till exempel om information om personer i e-post, på internet eller i en enkel lista som finns i datorn.

När missbruksregeln försvann innebär det att samma regler som finns för alla peson-uppgifter även ska gälla för det som skrivs om personer i exempelvis e-post och på webbplatser. Det innebär krav på att bland annat ha en rättslig grund, informera de registrerade, inhämta samtycke och föra register över vilka register som förs.

Den enskilda individen får en stärkt makt över sina personuppgifter genom rätten till insyn, till rättelser och ändringar. Om föreningen registrerar personuppgifter måste föreningen också informera de berörda om varför – på vilken rättslig grund – och hur länge informationen sparas. Informationen ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk.

Om föreningen lämnar personuppgifter till en annan organisation måste den organisationen också informeras då föreningen ändrar eller raderar personuppgifter. Det kommer inte att vara tillåtet att samla in och behandla fler uppgifter än nödvändigt för ändamålet, så kallad dataminimering.

Högre krav ställs nu på it-säkerhet. Om något händer, exempelvis att ett register kommer i orätta händer eller uppgifter skickas till fel mottagare, måste det finnas beredskap för att upptäcka, rapportera och utreda sådana incidenter. För känsliga uppgifter gäller att incidenterna måste rapporteras inom 72 timmar till Datainspektionen och till den/de registrerade.

Sanktionsavgifter införs. 20 miljoner euro eller fyra procent av företagets eller organisationens omsättning om det är en allvarlig överträdelse. 10 miljoner euro eller två procent av omsättningen i mindre allvarliga fall. Även enskilda personer kan begära skadestånd.

Vad behöver föreningen göra?

1. Informera alla i styrelsen om vad GDPR innebär och vad som kommer att gälla. Även om föreningen inte hanterar registren själv utan har en ekonomisk förvaltare eller annan förvaltare så finns det skäl att 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.

2. Inventera: Vilka register för vi och på vilken laglig grund? 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? Dokumentera det som kommer fram. Ett krav är att den som för uppgifterna ska kunna visa att reglerna följs. Bostadsrättsföreningar har laglig grund att föra lägenhetsregister och medlemsförteckning (bostadsrättslagen 9 kap. 8 §, samt lagen om ekonomiska föreningar 3 kap. 6§-8§). Har medlemmarna fått information om det och om hur länge data sparas?

3. Inhämta samtycke: 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. Granska befintliga samtycken: I de fall föreningen redan inhämtat samtycken, exempelvis för att publicera bilder eller annan information på sin webbplats, bör den se över hur dessa är utformade. Individen måste aktivt ha gett sitt samtycke efter att ha fått tydlig information. Kanske behöver nya samtycken inhämtas? Använd då gärna kryss- eller klickrutor eller underskrifter så att det blir tydligt att personen aktivt samtycker.

5. Se till att det finns rutiner för hur personuppgifter lämnas ut på begäran: Enskilda individer kommer att få en större möjlighet att begära ut, ändra och radera sina egna personuppgifter. Om PUL redan i dag följs är det en bra grund att utgå ifrån. Har föreningen en ekonomisk förvaltare som sköter detta behöver föreningen ändå ha koll på att det sköts på rätt sätt, att det finns rutiner för att till exempel rätta felaktiga uppgifter och även rätta dem hos annan organisation som fått uppgifter. Hur ser personuppgiftsbiträdesavtalet ut? Finns beredskap ifall en incident inträffar? Hur ser avtalen för molntjänster ut? Finns molntjänstleverantörens servrar utanför EU? Det behöver föreningen ha koll på eftersom överföring av uppgifter till tredje land bör begränsas.

Tänk på att inte

- Ha mer information i registren än vad lagen kräver, eller som är nödvändigt för att föreningen ska kunna fullgöra sina skyldigheter.

- Föra in några uppgifter som klassas som känsliga i registren i onödan, och i så fall ha en laglig grund eller samtycke för att föra sådana uppgifter (se känsliga personuppgifter).

Begrepp

*GDPR: General Data Protection Regulation

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. De fysiska personerna kan vara bostadsrättshavare, hyresgäster som är fysiska personer, kontaktpersoner hos lokalhyresgäster, anställda hos förvaltare, byggbolag, leverantörer och samarbetspartners, och andra.

PERSONUPPGIFTSBEHANDLING: Varje åtgärd som görs med personuppgifter, exempelvis att samla in och använda uppgifterna eller lämna ut dem till utomstående. Det kan till exempel vara avgifts- och hyresavisering, medlemsregistrering eller pantsättningsnotering. Behandling är det också om det handlar om passiva åtgärder som till exempel lagring av personuppgifter i it-system.

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, hostingtjänst m.m.

KÄNSLIGA PERSONUPPGIFTER: Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och uppgifter som rör hälsa och sexualliv. Även personuppgifter som rör lagöverträdelser som innefattar brott. Hanteringen av sådana uppgifter ställer högre krav, till exempel på kryptering/pseudonymisering. Utgångspunkten är att det är förbjudet att behandla sådana personuppgifter. Exempel på känsliga uppgifter i en förening kan vara ritningar som visar handikappanpassning i lägenhet och som lagts till lägenhetsregistret.

Källor till detta dokument Bostadsrätterna, Datainspektionens webbplats