Riksbyggen
Rum för hela livet

GDPR-info

Inledning

Nya regler för personuppgiftshantering

Från och med 25 maj 2018 gäller en ny EU-förordning som reglerar hur man får hantera personuppgifter. Dess engelska namn är General Data Protection Regulation, förkortas GDPR, och dess svenska är dataskyddsförordningen, förkortas DSF. I denna skrift används fortsättningsvis GDPR då det blivit den vanligaste benämningen på förordningen även i Sverige. GDPR ersätter den svenska personuppgiftslagen (PuL).

Genom GDPR vill man ge enskilda individer kontroll över hur deras personuppgifter hanteras och skapa enhetliga regler inom EU. GDPR innebär inte något generellt förbud mot att behandla personuppgifter utan reglerar under vilka förutsättningar man får behandla personuppgifter. Brott mot GDPR kan leda till höga sanktionsavgifter.

Nedan ges kortfattad information om vad en bostadsrättsförening bör tänka på i sitt förberedelsearbete inför GDPR. Mer information finns i en längre skrift som Riksbyggen tagit fram samt på Datainspektionens hemsida **www.datainspektionen.se**. På nästa sida finns en ordlista över grundläggande begrepp och en checklista för förberedelsearbetet.

Förberedelser

Kontroll över personuppgiftsbehandlingar

Alla som behandlar personuppgifter måste ha kontroll över sina behandlingar och säkerställa att behandlingarna sker i enlighet med GDPR. Det räcker inte bara att man gör rätt utan man måste också kunna bevisa för tillsynsmyndigheten att man gör rätt. Därför är det viktigt att dokumentera sitt personuppgiftsarbete. Alla som regelbundet behandlar personuppgifter måste också upprätta ett register över sina behandlingar – ett behandlingsregister. Bostadsrättsföreningar omfattas av denna skyldighet.

Kartläggning över behandlingar

För att kunna upprätta behandlingsregistret och bedöma om personuppgiftsbehandlingarna är lagliga måste man veta vilka personuppgifter som behandlas och varför man behandlar dem. Det är inte bara personuppgifter som finns i traditionella register eller förteckningar som omfattas av GDPR utan så snart en uppgift helt eller delvis behandlas digitalt och kan kopplas till en person så omfattas den. Utöver uppgifter i traditionella register omfattas därmed även exempelvis uppgifter i mail och utskrivna dokument.

Uppgiftsminimering och bevarandetid

En grundprincip i GDPR är uppgiftsminimering. Den innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, så kallade ”bra-att-ha-uppgifter”. Uppgifterna får inte heller behandlas om de till exempel är så gamla att de inte längre är relevanta för de ursprungliga ändamålen. Behandla endast personuppgifter som föreningen verkligen behöver och undvik i möjligaste mån att behandla känsliga personuppgifter.

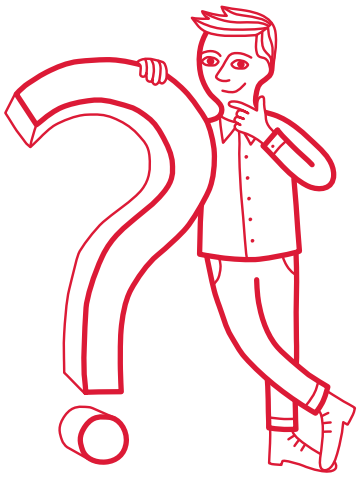
Personuppgifter får bara sparas så länge de är nödvändigt för de specifika ändamål för vilka de samlades in. Uppgifter som inte längre behövs ska gallras bort.

Laglig grund

För att personuppgifterna ska få behandlas måste det alltid finnas lagligt stöd i GDPR, en så kallad laglig grund. I GDPR finns ett antal lagliga grunder angivna. Exempel på lagliga grunder är samtycke från den registrerade, behandlingar som behövs för att fullgöra avtal med den registrerade och intresseavvägning. Det kan ibland vara svårt är att avgöra vilken laglig grund som gäller i ett specifikt fall men varje behandling måste ha en laglig grund. Saknas laglig grund måste föreningen radera uppgifterna och upphöra med behandlingen.

Behandlingar som utförs av andra

Innan GDPR träder i kraft måste bostadsrättsföreningen ingå (nya) personuppgiftsbiträdesavtal med de personuppgiftsbiträden föreningen använder sig av. Personuppgiftsbiträden kan vara allt från



molntjänstleverantörer till fastighetsförvaltare. Under våren kommer Riksbyggen skicka ut nya biträdesavtal till alla kunder men föreningen behöver även säkerställa att biträdesavtal finns med i, förekommande fall, andra personuppgiftsbiträden.

De registrerades rättigheter

De registrerade ska informeras om behandlingarna där deras personuppgifter förekommer och har rätt att få felaktiga uppgifter rättade. Under vissa förutsättningar har de också rätt att få uppgifter raderade eller blockerade samt att få ut och använda sina personuppgifter på annat håll, till exempel i en annan social medietjänst.

Information om behandlingarna ska lämnas dels vid insamling av uppgifter, dels efter begäran från registrerade. För behandlingar som pågår vid GDPR:s ikraftträdande kan ny information behöva lämnas till de registrerade och för behandlingar som grundas på samtycken behöver nya samtycken inhämtas.

Informationssäkerhet

Genom GDPR stärks kraven på informationssäkerhet. Alla som behandlar personuppgifter ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna. Personuppgifterna ska skyddas så att de inte stjäls eller oavsiktligt raderas, ändras eller sprids.

Personuppgiftsincidenter

Eventuella dataintrång eller andra former av förlorad kontroll över personuppgifter, så kallade personuppgiftsincidenter, måste dokumenteras. Ett tappat USB-minne som innehåller personuppgifter eller att någon obehörigen tagit del av personuppgifter är exempel på incidenter. Incidenter ska anmälas till Datainspektionen inom 72 timmar förutsatt att det inte är osannolikt att incidenten medför risker för den registrerades fri- och rättigheter. Om incidenten kan leda till att någon registrerad utsätts för allvarliga risker såsom ID-stöld, finansiella stölder eller diskriminering måste berörda registrerade dessutom informeras om händelsen så att de kan vidta nödvändiga åtgärder.

Utbildning

Bostadsrättsföreningen måste se till att alla i föreningen som kommer i kontakt med personuppgifter för föreningens räkning har grundläggande kunskaper om hur personuppgifterna ska hanteras.

Grundläggande begrepp

Personuppgifter

Med personuppgift avses all information som kan kopplas till en levande fysisk person. Både uppgifter som direkt kan knytas till personen (exempelvis namn och personnummer) och uppgifter som indirekt via annan information kan knytas till personen (exempelvis lägenhetsnummer, tvättstugebokningar, passageloggar i nyckelsystem) är personuppgifter. Även bilder och ljudupptagningar som lagras elektroniskt kan vara personuppgifter.

Vissa personuppgifter har ett starkare skydd i GDPR. Det handlar om så kallade känsliga personuppgifter som till exempel personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter om hälsa och sexualliv, samt personuppgifter som rör lagöverträdelser som innefattar brott. Även personnummer kan räknas till personuppgifter som är särskilt integritetskänsliga.

Den registrerade

Den som man behandlar personuppgifter om kallas den registrerade.

Behandling

Med behandling avses lite förenklat all form av befattning med en personuppgift och oberoende av om den sker automatiserat eller inte. Det kan vara fråga om insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgiftsansvarig

Den som bestämmer ändamålen med och medlen för behandlingen av en personuppgift är personuppgiftsansvarig.

Personuppgiftsbiträde

Den personuppgiftsansvarige kan anlita någon annan som behandlar personuppgifter för dennes räkning. Den som anlitas kallas personuppgiftsbiträde och finns alltid utanför den personuppgiftsansvariges organisation.

Behandlingsregister

Både personuppgiftsansvariga och personuppgiftsbiträden ska föra register över sina personuppgiftsbehandlingar. I GDPR anges vilka uppgifter som ska finnas med i registret.

Checklista

- Kartlägg alla personuppgiftsbehandlingar och upprätta ett behandlingsregister
- Ta bort alla personuppgifter som inte alls eller inte längre behövs
- Gör laglighetsbedömningen och sluta behandla eventuella uppgifter som saknar lagligt grund
- Informera de registrerade om era behandlingar och säkerställ att registerutdrag kan lämnas
- För behandlingar som sker med stöd av samtycke – inhämta nya samtycken vid behov
- Se till att personuppgiftsbiträdesavtal finns med alla som behandlar personuppgifter för föreningens räkning
- Ta fram en policy för bostadsrättsföreningens hantering av personuppgifter inklusive hur incidenter ska hanteras
- Se till att de inom bostadsrättsföreningen som hanterar personuppgifter har grundläggande kunskaper om GDPR