Dataskyddsförordningen i korthet

Den 25 maj 2018 ersätts personuppgiftslagen (PUL) av en ny dataskyddsförordning (även kallad ”GDPR” efter förordningens engelska namn, *General Data Protection Regulation*). Dataskyddsförordningen blir gällande lag i Sverige och inom EU/EES. Dessutom kommer en svensk dataskyddslag att träda ikraft samtidigt med förordningen. Personuppgifter behandlas i fastighetsföretags uthyrnings-och förvaltningsverksamhet men också i andra delar av verksamheten, till exempel vid kamerabevakning.

Nedan förklaras de begrepp som är viktiga att förstå för att du ska kunna kontrollera att bostadsrättsföreningen följer de krav som ställs i förordningen.

CENTRALA BEGREPP

Personuppgifter

All slags information som antingen direkt eller indirekt (det vill säga via annan information) kan kopplas till en fysisk person – såsom namn, lägenhetsnummer, IP-adress, fotografier, ljudfiler, beteenden, preferenser, uppgifter om störningar, löneuppgifter och uppgifter om utbildning. De personer som bostadsrättsföreningen behandlar personuppgifter om kan till exempel vara anställda, inhyrda konsulter, hyresgäster eller medlemmar som är fysiska personer eller enskilda firmor, kontaktpersoner hos hyresgäster som är företag, anställda hos förvaltare, byggbolag, leverantörer och samarbetspartners.

Behandla personuppgifter

Allt som vi gör med personuppgifter är en behandling. Exv. samla in, registrera, läsa eller gallra. Det kan vara helt eller delvis digitalt eller analogt (papper).

Personuppgiftsbehandling

Med personuppgiftebehandling menas exv. våra IT-system, word- och excelregister, e-postsystem eller pärmar med register.

Personuppgiftsansvarig

Den som bestämmer ändamålen och medlen för en personuppgiftsbehandling och därmed är ansvarig för att

behandlingen sker i enlighet med gällande rätt. Det är ett företag eller en organisation, inte en fysisk person, som avses.
I vårt fall innebär det att BRF Tonbadet 2 är personuppgiftsansvarig.

Personuppgiftsbiträde
Ett företag eller organisation som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige och för dennes räkning, exempelvis en tjänsteleverantör som inom ramen för sin leverans får tillgång till personuppgifter. Det kan vara en IT-leverantör eller ett anlitat bolag med uppdrag att sköta förvaltningen av en fastighet.

Känsliga personuppgifter
Personuppgifter som till exempel avslöjar etniskt ursprung, medlemskap i fackförening eller uppgifter om hälsa är att betrakta som känsliga personuppgifter. En uppgift om att någon behöver ett anpassat boende på grund av en funktionsnedsättning är ett exempel på en sådan känslig uppgift.

Registrerad
Med registrerad menas alla de personer som nämns i föreningens personuppgiftsbehandlingar. Det kan vara bostadsrättsinnehavare, hyresgäst, styrelsemedlem, kontaktperson för våra leverantörer och anlitade bolag.

GRUNDLÄGGANDE PRINCIPER

För att personuppgifter ska behandlas i enlighet med Dataskyddsförordningen måste ett antal grundläggande principer följas.

Ändamålsbegränsning
Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål (syfte). Det innebär kortfattat en skyldighet för den personuppgiftsansvarige att bara behandla personuppgifter för ändamål som objektivt sett kan anses vara berättigade och väl förankrade i verksamheten. Personuppgifterna får inte användas till annat än vad syftet angavs när de samlades in.

Laglighet, korrekthet och öppenhet
Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Kravet på att behandlingen av personuppgifter ska vara laglig innebär bland annat att det måste finnas en rättslig grund för behandlingen.

Att personuppgifter ska behandlas på ett öppet sätt innebär bland annat att det ska vara klart och tydligt för den registrerade hur hans eller hennes personuppgifter samlas in och behandlas. De registrerade har därför rätt till information om behandlingen som är

både lättillgänglig och har formulerats med ett klart och tydligt språk.

Lagringsminimering (gallring)
Som huvudregel får personuppgifter inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När de inte behövs längre ska de tas bort. Det är behovet som styr när personuppgifter ska gallras. Finns det någon lagstiftning som anger att informationen ska bevaras på individnivå, till exempelvis för bokföringsändamål, är det tillåtet.

Integritet och konfidentialitet
Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Uppgiftsminimering
Det är inte tillåtet att samla in fler personuppgifter än nödvändigt. Alla uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de angivna ändamålen.

Ansvarsskyldighet
Den som behandlar personuppgifter ska kunna visa att dataskyddslagstiftningen följs.
Det kräver som regel en kartläggning och dokumentation av alla behandlingar av personuppgifter i en så kallad registerförteckning. Dessutom kan styrande dokument, skriftliga riktlinjer, IT-säkerhet och en väl utvecklad organisation kring dataskyddsfrågor, visa detta.

Säkerhet
Personuppgifter ska skyddas på ett sätt som är lämpligt med hänsyn till hur skyddsvärda de är och hur stor risken är att de kan missbrukas. Känsliga personuppgifter kräver alltså ett högre skydd än andra.

Inbyggt dataskydd och dataskydd som standard
Inbyggt dataskydd innebär att hänsyn tas till dataskyddslagstiftningen redan när IT-system och arbetsrutiner utformas. Kravet på dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan.

LAGLIG GRUND

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett uttryckligt stöd i Dataskyddsförordningen – en laglig grund.

De lagliga grunder som används är:

- samtycke från den registrerade
- nödvändigt för att fullgöra ett avtal med den registrerade (hyresavtal/bostadsrättsavtal)
- fullgöra en rättslig förpliktelse
- skydda den registrerades grundläggande intressen
- efter en intresseavvägning

VILL DU VETA MER?

Datainspektionen är tillsynsmyndighet i Sverige och på deras hemsida finns mer information att läsa om du är intresserad: www.datainspektionen.se

Du kan också ställa frågor till styrelsen genom att skicka ett mail till styrelsen@brftonbadet2.se

känslig uppgift.

Registrerad
Med registrerad menas alla de personer som nämns i föreningens personuppgiftsbehandlingar. Det kan vara bostadsrättsinnehavare, hyresgäst, styrelsemedlem, kontaktperson för våra leverantörer och anlitade bolag.

1. GRUNDLÄGGANDE PRINCIPER

För att personuppgifter ska behandlas i enlighet med Dataskyddsförordningen måste ett antal grundläggande principer följas.

Ändamålsbegränsning
Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål (syfte). Det innebär kortfattat en skyldighet för den personuppgiftsansvarige att bara behandla personuppgifter för ändamål som objektivt sett kan anses vara berättigade och väl förankrade i verksamheten. Personuppgifterna får inte användas till annat än vad syftet angavs när de samlades in.

Laglighet, korrekthet och öppenhet
Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Kravet på att behandlingen av personuppgifter ska vara laglig innebär bland annat att det måste finnas en rättslig grund för behandlingen.

Att personuppgifter ska behandlas på ett öppet sätt innebär bland annat att det ska vara klart och tydligt för den registrerade hur hans eller hennes personuppgifter samlas in och behandlas. De registrerade har därför rätt till information om behandlingen som är både lättillgänglig och har formulerats med ett klart och tydligt språk.

Lagringsminimering (gallring)
Som huvudregel får personuppgifter inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När de inte behövs längre ska de tas bort. Det är behovet som styr när personuppgifter ska gallras. Finns det någon lagstiftning som anger att informationen ska bevaras på individnivå, till exempelvis för bokföringsändamål, är det tillåtet.

Integritet och konfidentialitet
Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Uppgiftsminimering
Det är inte tillåtet att samla in fler personuppgifter än nödvändigt. Alla uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de angivna ändamålen.

Ansvarsskyldighet
Den som behandlar personuppgifter ska kunna visa att dataskyddslagstiftningen följs.
Det kräver som regel en kartläggning och dokumentation av alla behandlingar av personuppgifter i en så kallad registerförteckning. Dessutom kan styrande dokument, skriftliga riktlinjer, IT-säkerhet och en väl utvecklad organisation kring dataskyddsfrågor, visa detta.

Säkerhet
Personuppgifter ska skyddas på ett sätt som är lämpligt med hänsyn till hur skyddsvärda de är och hur stor risken är att de kan missbrukas. Känsliga personuppgifter kräver alltså ett högre skydd än andra.

Inbyggt dataskydd och dataskydd som standard
Inbyggt dataskydd innebär att hänsyn tas till dataskyddslagstiftningen redan när IT-system och arbetsrutiner utformas. Kravet på dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan.

2. LAGLIG GRUND

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett uttryckligt stöd i Dataskyddsförordningen – en laglig grund.

De lagliga grunder som används är:

- samtycke från den registrerade
- nödvändigt för att fullgöra ett avtal med den registrerade (hyresavtal/bostadsrättsavtal)
- fullgöra en rättslig förpliktelse
- skydda den registrerades grundläggande intressen
- efter en intresseavvägning

3. VILL DU VETA MER?

Datainspektionen utövar tillsyn över dataskyddslagstiftningen och på deras hemsida finns mer information om
www.datainspektionen.se