POLICYDOKUMENT GDPR

Fortinova AB

Fortinova Fastigheter AB (publ)

Policydokumentet inbegriper ovanstående bolags dotterbolag

2018-05-23

Innehåll

Bakgrund

Vad är GDPR?

GDPR står General Data Protection Regulation och är EU:s nya dataskyddsförordning vilken börjar gälla som svensk lag från den 25 maj 2018. Lagen reglerar hur företag och organisationer ska behandla personuppgifter där sanktionsavgifterna är kännbara om man inte följer den. Det nya regelverket ersätter personuppgiftslagen (PuL) och delvis även patientdatalagen (PDL). Tillsynsmyndighet för att se till att reglerna efterföljs är Datainspektionen.

Det huvudsakliga syftet med dataskyddsförordningen är att skydda de enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Rätten till privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Dataskyddsförordningen har också till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras. Detta innebär att samma regler ska gälla inom hela EU. Dock har Sverige, tillskillnad från de flesta EU-länder, ett historiskt arv i form av offentlighetsprincipen som i vissa fall kan upplevas ha motsatta syften.

GDPR beskrivs i följande grundläggande sex principer:

1. Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

2. Insamlingen av personuppgifter ska vara begränsad till ändamålet och ske för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte senare användas för ett ändamål som inte är bundet till ändamålet med de insamlade uppgifterna.

3. Insamlingen av personuppgifter ska vara uppgiftsminimerad, dvs. inte för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas, och uppgifterna ska vara adekvata och relevanta.

4. Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Den personuppgiftsansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är inexakta och felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

5. Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas. Uppgifter får dock förvaras längre, om de endast behandlas för arkivändamål av allmänt intresse, eller används för historiska forskningsändamål eller statistiska ändamål.

6. Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna och därmed uppgifternas integritet och konfidentialitet. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Då ska lämpliga tekniska eller organisatoriska åtgärder användas.

Denna policy ska därför vara en grund att kunna leva upp både till dataskyddsförordnigen och säkerställa en korrekt hantering av allmänna handlingar enligt den svenska offentlighetsprincipen.

Varför ett policydokument?

Då ett normalt fastighetsbolag behandlar diverse personuppgifter innebär det nya regelverket inte nödvändigtvis stora eller omgripande förändringar. Vår bedömning är dock att ett övergripande arbete för att säkerställa rutiner är nödvändigt.

Detta dokument fungerar som en sammanfattning och ett ställningstagande av de slutsatser som kunnat dras av arbetet.

Begreppet personuppgift

Personuppgifter enligt GDPR är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Uppgifter som hänförs till en juridisk person såsom en leverantör i bolagsform är därmed ingen personuppgift enligt denna definition. Detta kan vara namn, personnummer, ljudupptagningar och bilder men också sådana uppgifter som indirekt kan kopplas till fysiska personer. Exempel på sådana uppgifter kan vara registreringsnummer på bilar, adresser, lägenhetsnummer och IP-adresser. Kan de inte kopplas till en fysisk person räknas de därmed inte som en personuppgift.

Känsliga personuppgifter

Känsliga personuppgifter enligt GDPR omfattar:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- genetiska uppgifter och biometriska uppgifter för att entydigt identifiera en fysisk person
- uppgifter om hälsa
- uppgifter om en fysisk persons sexualliv eller sexuella läggning

Bedömningen är att bolagen i ytterst liten utsträckning hanterar känsliga personuppgifter enligt de definitioner som presenteras ovan. Dessa avser normalt uppgifter i form av hälsa såsom sjukfrånvaro och graviditeter som ett led i att kunna fullgöra de krav som finns i anställningsavtalen.

Utöver sådana personuppgifter som klassificeras som känsliga kan ändå personuppgifter som kan anses som integritetskänsliga uppgifter hanteras i bolagens verksamheter. Sådana uppgifter kan vara störningsärenden, skadedjur, felparkeringar, inkomstuppgifter mm.

Att hantera personuppgifter

Att spara personuppgifter

Enligt dataskyddsförordningen får den personuppgiftsansvarige behandla personuppgifter om de uppfyller ett antal olika krav. De som är mest aktuella för våra bolags verksamhet bedöms vara:

- behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås
- behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige
- den registrerade har lämnat sitt samtycke

Bolagens ambition ska vara att minimera insamlandet av personuppgifter och att sådana uppgifter som inte är nödvändiga för att fullgöra åtaganden enligt hyresavtal eller andra ingångna överenskommelser inte skall sparas. System och processer som hanterar personuppgifter har vid GDPRs införande genomgåtts, dokumenterats och nödvändiga rensningar genomförts. System och processer skall sedan löpande revideras och utvecklas för att säkerställa en så korrekt och rättssäkerhetsmässig hantering som är möjlig.

De personuppgifter som insamlas skall hanteras säkert och inte användas till andra ändamål än vad de är avsedda för. Endast personal som är av behov av information skall ha åtkomst till dessa. Exempel på detta kan vara uppgifter om frånvaro och sjukdom som ska begränsas till de personer som handlägger löner.

För personuppgifter som insamlas där det inte finns lagligt eller avtalsenligt stöd skall medgivande för insamlandet av sådan information inhämtas från den enskilda innan personuppgifterna lagras. Information hur den enskilde kan tillvarata sina rättigheter och begära att personuppgifter utrangeras skall finnas lätt tillgängligt enligt lagar, rekommendationer och praxis. Exempel på sådana situationer kan vara vid anmälan till lägenhet eller bostadskö som sker frivilligt.

Åtaganden enligt hyreslagen

Hyreslagens krav och hyresgästens förväntningar på hyresvärden är vida varför vår bedömning är att det är nödvändigt att behålla relativt stora mängder information om boendet, de boende och förhållanden inom fastighetsbeståndet.

Hyresvärdens grundläggande skyldighet är att ställa en lägenhet i användbart skick till hyresgästens förfogande. Hyresgästens skyldighet är sedan att använda lägenheten som man avtalat, att hyran betalas i rätt tid, att lägenheten vårdas väl och att grannar inte störs.

För hyresvärdens fullgörande av dessa åtaganden krävs god ordning avseende inkomna felanmälningar, störningsärenden, uppföljning av betalda avier inklusive eventuell kravhantering mm och vidare krävs att personuppgifter sparas för att till exempel åtgärda rapporterade felanmälningar, anmodan att vidtaga rättelse, kontroll på utlämnade nycklar mm.

Information om historiska felanmälningar behövs därför t.ex. sparas för att vi som hyresvärdar även i framtiden skall kunna fullgöra våra åtaganden. Sådan information som insamlas för att

fullgöra avtalsenliga förhållanden enligt hyreslagen kräver därmed inte att den enskilde i förväg ger sitt medgivande.

Annan lagstiftning och offentlighetsprincipen

Annan lagstiftning kräver också att information sparas såsom bokföringslag och årsredovisningslagen. Då information som sparas enligt annan lag inte kräver den enskildes medgivande skall sådan information sparas som är tillräcklig för att fullgöra de lagmässiga krav som kan ställas från myndigheter, revisorer eller andra.

Ställningstaganden

Bolagsgemensamma ställningstaganden

Bolagen har gjort bolagsindividuella inventeringar av system och processer där personuppgifter insamlas och registreras. Ett antal sådana processer finns i samtliga bolag och kan ses som branschövergripande insamling. Exempel på sådana processer är:

- Hyressystem inklusive avtal, avisering och kravhantering
- Affärssystem för bokföring
- Lägenhetskö
- Låssystem/passersystem/larm
- Personalsystem inklusive lönehantering
- Ärendehantering
- Styr/övervakning av drift

Återkommande för dessa processer är att de är nödvändiga för att fullfölja de avtal som tecknats oavsett de avser hyresavtal, anställningsavtal eller leveransavtal/ramavtal. Undantag avser lägenhetskö. Vår bedömning är därför att för sådana processer krävs inget i förväg medgivande från hyresgäster, anställda eller leverantörer. Loggar och ärenden bör därför sparas över tid för att säkerställa en långsiktigt säkert och tryggt boende. Detta innebär också att vår bedömning är att t.ex. loggar för in- och utpassager är nödvändiga för att säkerställa trygghet i våra bostadsområden. Man kan på detta sättet även i efterhand kontrollera vilka som passerat vid störningsmoment i gemensamma utrymmen.

I möjligaste mån bör direkta personuppgifter såsom namn och personnummer utrangeras i för sådana processer där det är lägenheten eller fastigheten som över tid behöver följas. Exempel på sådant är ärendehantering och styr/övervakning av drift.

För personuppgifter som insamlas för direkta beslut bör sådana utrangeras då ärendet är stängt. Exempel på sådana uppgifter är information om inkomst i samband med prövning av huruvida ett hyresavtal bör tecknas med en enskild. Då avtal är tecknat bör sådan information utrangeras snarast efter den tidpunkt då handläggaren bedömer att informationen inte är nödvändig längre.

Bolagsindividuella insatser

Varje bolag ska genomföra individuella inventeringar och dokumentera dessa i en registerförteckning. Exempel på rubriker som bör ingå i respektive bolags registerförteckning:

- Typ av system och/eller process
- Vilka typer av personuppgifter registreras
- Förekommer känsliga personuppgifter och vilka?
- Motivering till varför personuppgifter sparas? (laglig eller avtalsmässig grund)
- Ange laglig eller avtalsmässig grund
- Bedömning av behov av samtycke
- Tidsfrist för radering/utrangering
- Om överföring sker till tredje land (icke EU)
- Om personuppgiftsbiträde anlitas

Dataskyddsombud

Vår bedömning är att våra bolag inte behöver utse ett dataskyddsombud.

Personuppgiftsansvarig

Personuppgiftsansvarig är normalt den juridiska person som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Det är alltså ingen specifik person eller position i bolaget som är personuppgiftsansvarig.

Om verksamheten bedrivs i en koncern kan ansvarsfördelningen se ut på olika sätt.

- Om moderbolaget ensamt bestämmer över behandlingen blir moderbolaget personuppgiftsansvarig.
- Om alla bolag inom en koncern gemensamt bestämmer över behandlingen blir de tillsammans ansvariga för det aktuella registret

Vår bedömning är att det är den juridiska personen i form av aktiebolag som blir personuppgiftsansvarig.

Enligt dataskyddsförordningen ska den personuppgiftsansvarige ansvara för att principer och krav efterlevs samt ansvara för att, t.ex. vid en extern granskning, kunna visa att principerna och kraven har efterlevts. Den personuppgiftsansvarige ansvarar också för bedömningar av vad principerna innebär i det vardagliga praktiska arbetet och dokumentera dessa bedömningar. Den personuppgiftsansvariga ska därmed genomföra lämpliga åtgärder såväl tekniskt rörande system etc och åtgärder som rör organisationen som hanterar personuppgifter. Detta kan innebära utbildning av personalen, att ta fram interna anvisningar, säkerställa avtal, övervakning och uppföljning av konton och tekniska begränsningar av åtkomst i system.

Hantering av e-post

E-post innebär normalt att man alltid behandlar personuppgifter. Själva e-postadressen i sig är oftast en personuppgift och all annan information i meddelandet som kan kopplas till en enskild person är också personuppgifter. Hantering av e-post ska därför finnas med i den av enskilda bolaget upprättade registerförteckningen och ska uppfylla krav i dataskyddsförordningen. Det som skiljer e-post från andra inkomna handlingar är att innehållet normalt är okänt när handlingen inkommer.

Personuppgiftsbiträdesavtal

Den som använder en extern leverantör, t.ex. i form av molntjänster, för behandling av personuppgifter är personuppgiftsansvarig trots att den utförs av den externa leverantören. Leverantören, och alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden. Det är den personuppgiftsansvarige som ansvarar för att lagar och egna regelverk följs.

Innan t.ex. en molntjänst tas i bruk måste den personuppgiftsansvarige bedöma om den personuppgiftsbehandling som man vill låta molntjänstleverantören utföra kommer att vara tillåten enligt lagstiftningen. Personuppgiftsbiträden får bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Normalt utformar den personuppgiftsansvarige själv instruktionerna, t.ex. i ett personuppgiftsbiträdesavtal.

Den personuppgiftsansvarige måste därför säkerställa att alla externa leverantörer som hanterar personuppgifter följer de instruktioner som finns och därmed upprätta personuppgiftsbiträdesavtal.

Dina rättigheter

Som registrerad hos Fortinova har du rätt att få dina personuppgifter korrigerade om de är felaktiga. Om du använder dig av Mina sidor görs ändringen enklast där. I annat fall kontaktar du kundtjänst. Du har också rätt att veta hur dina personuppgifter används i vår verksamhet och vilka uppgifter vi behandlar.

Sammanfattning

Bolagens sammanfattande bedömning är att den övervägande andelen av personuppgifter som sparas har laglig eller avtalsmässig grund. Personuppgifter som sparas rörande personal är i huvudsak kopplade till att kunna fullgöra villkor som regleras i anställningsavtal och de lagar som rör anställd personal. Personuppgifter som rör hyresgäster sparas för att fullgöra hyresavtal och de åtaganden som bolagen har som hyresvärdar. I detta ingår också åtaganden som rör behovet av ett tryggt och säkert boende. De personuppgifter som hanteras inom ramen för bokföringen sparas i enlighet med bokföringslagen och har därmed laglig grund. För sådana personuppgifter som inte är kopplade till ett specifikt avtal såsom anmälan till lägenhetskö skall medgivande inhämtas innan registrering sker.

Bolagens bedömning är därmed att de personuppgifter som sparas följer den nya dataskyddsförordningen och dess andemening. Huvuduppgiften för bolagen är att under tid säkerställa en korrekt hantering, att överinformation inte sparas, att utrangering av information genomförs och informationen endast används till det de är avsedda att användas.

Varje bolag har i detta arbete genomfört en inventering och registerförteckning för att säkerställa den ovan beskrivna bedömningen. Bolagen kommer också arbeta med att säkerställa att rätt personer hanterar de uppgifter de behöver hantera för att fullgöra sitt uppdrag och att de har rätt utbildning och funktionsdugliga instruktioner.