KÄVLINGE KOMMUN

Kommunrevisionen

Presidiet Kommunstyrelse

Kävlinge kommun

Granskning av införandet av dataskyddsförordningen hos KKB

EY, har genomfört en granskning av införandet av dataskyddsförordningen hos KKB. Gjorda iakttagelser har sammanställts i bifogad rapport.

Ordförande i revisionen har haft samtal före och efter rapporten i syfte att få företaget (KKB) att ha en så bra start som möjligt med införande av den nya Dataskyddsförordningen per den 25 maj 2018. Målet är i sikte. Rapporten är enbart för överseende inget svar önskas.

Kävlinge kommuns revisorer

Fernando Dinis-Viseu
Ordförande

Kopia till:
Kanslichef Mats Svedberg

Kommunrevisionen
Namn
telefon • e-post

Kävlinge kommun
Kullagatan 2, 244 80 Kävlinge
046 - 73 90 00 • kommunen@kavlinge.se • www.kavlinge.se

Revisionsrapport 2018
Genomförd på uppdrag av lekmannarevisorerna
April 2018

Kävlinge kommun

Granskning av införandet av dataskyddsförordningen hos KKB Fastigheter AB

Building a better working world

Building a better working world

Innehåll

Building a better working world

1. Inledning

1.1. Bakgrund

Den 25 maj 2018 kommer den nya europeiska dataskyddsförordningen att ersätta den svenska personuppgiftslagen (PUL) och bli lag i Sverige. Förordningen innehåller regler om hur personuppgifter får behandlas av myndigheter. Det nya regelverket kan innebära stora förändringar för den kommunala verksamheten och dess bolag, vilket gör det angeläget med noggrann planering och förberedelse för anpassning till det nya regelverket. Det finns annars en risk att den enskildes personliga integritet kränks eller att kommunen/bolagen tvingas betala sanktionsavgifter, om reglerna inte följs.

1.2. Syfte och revisionsfrågor

Granskningens syfte är att bedöma om verkställande direktör och KKB Fastigheter AB:s styrelse arbetar på ett ändamålsenligt sätt med planering och anpassningar inför införandet av den nya dataskyddsförordningen.

I granskningen besvaras följande revisionsfrågor:

- Har styrelsen tydliggjort ansvaret?
- Har nödvändiga förändringar med anledning av införande av förordningen identifierats?
- Har nödvändiga anpassningar påbörjats i rimlig omfattning?
- Finns aktuella och ändamålsenliga rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheterna?
- Har nyckelpersoner i bolaget informerats om förändringarna och dess innebörd på ett tillräckligt sätt?

1.3. Genomförande

Granskningen grundas på intervjuer och dokumentstudier (se bilaga 1). Intervju har skett med marknadschefen, som har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd februari – mars 2018.

Building a better working world

2. Revisionskriterier

2.1. Dataskyddsförordningen

Dataskyddsförordningen blir, efter beslut i EU, svensk lag den 25 maj 2018 och ersätter därmed personuppgiftslagen (PUL) i Sverige. Dataskyddsförordningen reglerar, i likhet med PUL, grundläggande bestämmelser om enskildas rätt till skydd av personuppgifter. Att skydda enskildas grundläggande rättigheter och friheter kopplat till personuppgiftshantering är således ett av syftena med dataskyddsförordningen.

En stor del av bestämmelserna i dataskyddsförordningen överensstämmer med tidigare bestämmelser enligt PUL, men några viktiga förändringar finns. Nedan sammanfattas de huvudsakliga förändringarna för organisationer[1] i korthet.

- **Samtycke** – dataskyddsförordningen bygger i stor utsträckning på aktivt samtycke till registrering. I förordningen ställs särskilda krav på hur samtycke ska lämnas, i synnerhet vid behandling av känsliga personuppgifter (såsom uppgifter om hälsa eller religiös åskådning). Den som behandlar särskilt känsliga personuppgifter måste kunna visa att giltigt samtycke har lämnats av den som har registrerats.

- **Ökade rättigheter** – enligt dataskyddsförordningen har den registrerade rätt att när som helst begära att få sina uppgifter raderade, med undantag för om det föreligger någon rättslig grund för behandlingen. Undantagsfall kan uppstå i de fall organisationen som hanterar personuppgifter behöver dessa för exempelvis bokföringsändamål. Med tanke på de ökade kraven som ställs på att de registrerade enkelt ska kunna få sina uppgifter raderade bör organisationen enligt Datainspektionen se över rutiner gällande hur en sådan begäran hanteras.

- **Dataportabilitet** – när uppgifter behandlas med stöd av samtycke eller för att uppfylla ett avtal, ska den registrerade ha rätt att få ut de uppgifter som lämnats för att överföra dem till en annan tjänst.

- **Konsekvensbedömning** – innan man planerar en ny personuppgiftsbehandling, vilken innebär särskilda risker för den registrerade, ska en bedömning göras av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska risker för den enskilde.

- **Anmälan om personuppgiftsincident** – vid händelse av säkerhetsincident, exempelvis dataintrång eller oavsiktlig förlust av uppgifter, måste det anmälas till Datainspektionen inom 72 timmar. Vid risk för exempelvis id-stöld eller bedrägeri kan de personer vars personuppgifter berörs behöva informeras.

- **Dataskyddsombud** – vissa organisationer, myndigheter eller andra former som behandlar känsliga uppgifter, eller är involverade i särskilt riskfylld behandling av personuppgifter, måste utse en person i organisationen som har som särskild uppgift att bevaka dataskyddsfrågor – ett dataskyddsombud. Ombudet har bland annat till uppgift att utföra kontroller och informationsinsatser. Ombudet ska vara väl insatt i de lagar som gäller för personuppgiftsbehandling.

[1] Dataskyddsförordningen gäller i princip inom all slags verksamhet och oavsett vem som utför personuppgiftsbehandlingen. Den gäller således för företag, föreningar, organisationer, myndigheter och privatpersoner. I detta avsnitt används begreppet organisation, vilket även innefattar kommuner.

- **"Missbruksregeln" försvinner** – när dataskyddsförordningen träder ikraft kommer den så kallade missbruksregeln inte längre finnas kvar. Missbruksregeln innebär att man idag kan använda enklare regler för personuppgifter i ostrukturerat material, exempelvis information om personer i e-post, på internet eller i en enkel lista som man har i datorn. När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på webbplatser.

- **Sanktionsavgift** – vid brytande mot förordningens regler kan Datainspektionen ålägga en sanktionsavgift. Avgiftens storlek är bland annat beroende av hur allvarlig överträdelsen är, om det skett avsiktligt eller inte samt vilka åtgärder som vidtagits för att minska skadan. Vid mindre förseelser riskerar den som bryter mot förordningen ett påpekande eller föreläggande om eventuella brister. Anses brottet däremot vara allvarligare, eller om organisationen anses ovillig att vidta nödvändiga åtgärder, riskeras böter upp till 20 miljoner euro eller 4 % av företagets/organisationens eller moderbolagets globala omsättning.

2.2. Datainspektionens vägledning

Datainspektionen är tillsynsmyndighet när det gäller kommunernas hantering av personuppgifter. Enligt Datainspektionens vägledning behöver kommunerna bl.a. förbereda sig inför Dataskyddsförordningens ikraftträdande på följande vis:

- Försäkra sig om att beslutsfattare och nyckelpersoner inom organisationen är medvetna om att personuppgiftslagen kommer att ersättas av dataskyddsförordningen. Undersöka hur organisationen kommer att påverkas av förordningen och identifiera de områden som de måste arbeta särskilt med.

- Inventera och dokumentera vilka personuppgifter som hanteras, hur de samlas in och till vem uppgifterna lämnas ut. Göra en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av organisationen.

- Undersöka om verksamheten har utnyttjat personuppgiftslagens undantag för att behandla personuppgifter i ostrukturerat material, den så kallade missbruksregeln. Denna regel kommer inte att finnas kvar i förordningen. Undersöka särskilt om behandling som idag stödjer sig på missbruksregeln är förenlig med dataskyddsförordningens bestämmelser.

- Granska den information som lämnas till de registrerade och fundera över vilka förändringar av den informationen som kan bli nödvändig att göra.

- Se över rutiner för att säkerställa att alla rättigheter som de registrerade har enligt dataskyddsförordningen kan uppfyllas, som exempelvis hur personuppgifter raderas och hur uppgifter lämnas ut elektroniskt i ett allmänt använt format.

- Undersöka vilka olika typer av uppgifter som behandlas och med vilket rättsligt stöd detta görs. Dokumentera slutsatserna.

- Undersöka på vilket sätt samtycke inhämtas, vilken information som lämnas och hur uppgiften om att samtycke har lämnats av den registrerade sparas.

- Se till att det finns tillräckliga rutiner på plats för att upptäcka, rapportera och utreda personuppgiftsincidenter.

- Fundera på om personuppgiftsbehandlingen är förenad med särskilda risker för enskildas fri- och rättigheter och om det i så fall behöver göras en konsekvensbedömning avseende dataskydd.

- Ta hänsyn till dataskyddsförordningens regler när nya IT-system tas fram eller befintliga förändras. Det ger en större möjlighet att följa reglerna, höja säkerheten och förhindra onödiga framtida kostnader.

- Bestämma var i organisationen som ansvaret för dataskyddsfrågor ska ligga. Även för de organisationer som inte måste utse ett dataskyddsombud, rekommenderar Datainspektionen att ett ombud utses om organisationen utför arbetsuppgifter av allmänt intresse.

Building a better working world

3. Iakttagelser

3.1. Ansvar och roller

Av intervjun med marknadschefen framkom att bolaget har varit medveten om dataskyddsförordningen sedan 2016, men att de har väntat med att besluta vem i organisationen som ska fokusera på frågan samt initiera utbildningar. Valet att vänta grundas på att det har funnits en otydlighet kring hur förordningen ska tolkas och lagstiftas nationellt. Marknadschefen uppdrogs i januari 2018 att sätta sig in i den nya förordningen och vad den ska komma att innebära för bolaget.

Vid styrelsens sammanträde den 6 mars 2018 informerades styrelsen om dataskydds-förordningen för första gången. Vid sammanträdet beslöt styrelsen att uppdra åt VD att vidta nödvändiga åtgärder för att säkerställa att bolagets behandling av personuppgifter följer den nya lagstiftningen samt att i förekommande fall utse ett dataskyddsombud. Bolaget har under granskningens genomförande utsett ett dataskyddsombud. Den verkställande direktören utsåg marknadschefen till bolagets dataskyddsombud.

Bolaget har beslutat att minska telefontiderna med fem timmar/vecka för att frigöra arbetstid från marknadschefen och från övriga fyra medarbetare i marknadsgruppen. Delar av marknadschefens befintliga arbetsuppgifter har delegerats till övriga medarbetare, så att marknadschefen kan driva bolagets GDPR-arbete.

Bolaget är en fristående personuppgiftsansvarig, vilket innebär att bolaget ansvarar för att säkerställa att behandling av personuppgifter inom den egna verksamheten sker i enlighet med lagstiftningen. Kommunen som ägare har därför inte varit delaktig eller ställt krav på att bolaget ska följa de strategier eller riktlinjer som kommunen avser att upprätta.

3.2. Identifiering av och påbörjade åtgärder

Bolaget har genomfört en inventering av vilka behandlingar av personuppgifter som är aktuella inom bolagets verksamhet. Bolaget har utgått från de processer där behandlingar av personuppgifter sker, vilka är; sökande, kund, personal, Justitia, Securitas, uppgifter via e-post. Vi har tagit del av ett utkast på en förteckning över ett register som avser behandling av personuppgifter vid registrering av intresseanmälan. I dokumentet återfinns följande rubriker med tillhörande information:

- Personuppgiftsansvarig
- Dataskyddsombud
- Databiträdesansvarig
- Ändamål med behandlingen
- Uppgifter som behandlas
- Rättslig grund för behandlingen
- Kategori av registrerade
- Kategori av personuppgifter
- Mottagare
- Tidsfrister för radering

Av intervjun framkom att liknande dokument ska arbetas fram för de övriga behandlingarna som angavs ovan. Det framkom även att bolaget planerar att samla samtliga register i ett gemensamt dokument som även kommer att innehålla en innehållsförteckning.

Bolaget har påbörjat samtal med leverantörer inför upprättandet av personuppgifts-biträdesavtal. Dessa är Vitec (hyresgäst- och sökandesystem), Agda/Visma (lönesystem), Securitas (säkerhetstjänster) och Justitia (kredithantering). Biträdesavtalen är ännu inte på plats men kontakten har varit till för att kontrollera vilka leverantörer som ska bekräfta hur bolagets uppgifter behandlas. I hyresgäst- och sökandesystemet (Vitec) finns möjligheten att göra utdrag på vilka behandlingar som gjorts av personuppgifter. Detta är en tjänst som leverantören har erbjudit sina kunder med anledning av dataskyddsförordningen. Tjänsten kan användas när privatpersoner begär ut information om vilka behandlingar som har gjorts av deras personuppgifter. Vi har tagit del av ett exempel på ett utdrag som redogör vilka personuppgifter som kan behandlas av bolaget.

Identifierade åtgärder är att ta fram planer för bevarande och gallring, adresshantering, hur störningsärenden[2] ska kunna dokumenteras utan att känsliga uppgifter röjs. Vidare måste en dataskyddspolicy arbetas fram som säkerställer att bolagets tekniska lösningar är säkerställda. Därtill ska bolaget revidera dokumenthanteringsplanen och policyn avseende registerhantering. Bolaget ska också se över uthyrningsprocessen för att identifiera i vilka led som behandling av personuppgifter sker.

En ytterligare åtgärd som behöver vidtas är att se över behörigheterna i bolagets olika system. Detta gäller lönesystemet, sökanderegistret och hyresgästregistret men främst det sistnämnda då samtliga som har behörighet till systemet ser alla uppgifter som finns. Det finns dock skillnader i behörigheten, då vissa har tittarbehörighet och andra har redigerarbehörighet. Vid granskningens genomförande har inga arbetsgrupper tillsatts för att påbörja de identifierade åtgärderna.

Bolaget har arbetat fram mallen Rapport personuppgiftsincident. I rapportmallen finns följande rubriker:

1. Situationshantering: fem steg som anger ordningen för att hantera situationen; vidta åtgärd om det kan göras på ett enkelt sätt, informera bolagets VD, berörda och biträde/leverantörer samt upprätta incidentrapporten.
2. Incidentrapporten avser: incident, säkerhetsrisk, driftavbrott
3. Information om/kring uppkommen situation
4. Bedömning av konsekvens och/eller risk: en 1-5 prioriteringskala (1 = högsta prioritet och 5 = lägsta prioritet), tillhörande beskrivning på tillvägagagångssättet beroende på bedömning.
5. Beskrivning av incident, säkerhetsrisk eller driftavbrott
6. Vidtagna åtgärder
7. Signering av incidentrapport

Bolaget har arbetat fram en tidplan som anger identifierade åtgärder och när i tid de ska genomföras. Tidplanen består av tre delfaser som är indelade i januari-februari, mars-april och slutligen maj. I tidplanen anges att arbetsgrupper ska utse till den 10 april och att regelbundna avstämningsmöten ska ske. De identifierade åtgärderna såsom gallring, översyn av behörigheter, förteckning över personuppgiftsregister samt revidera policys ska vara färdigställt till den 30 april. Av tidplanen framgår att dataskyddsombudet kommer att inrapporteras till Datainspektionen den 20 maj.

Bolaget inväntar den nya uppförandekoden som SABO ska ta fram tillsammans med Fastighetsägarna Sverige i enlighet med bestämmelserna i dataskyddsförordningen.

[2] När boende har ett klagomål som gäller en störning som de vill rapportera in till bolaget så upprättas ett störningsärende.

Uppförandekoden för personuppgiftsbehandling kommer att ersätta den nuvarande branschöverenskommelsen avseende personuppgiftslagen (PUL). Enligt uppgift är det uppförandekoden som kommer att ge bolaget den största vägledningen i implementeringen av förordningen. Det är Datainspektionen som ska godkänna de olika organisationernas uppförandekoder då myndigheten tillträtt som tillsynsmyndighet den 25 maj 2018. Datainspektionen har dock informerat bolagen om att de inte kommer att prioritera denna uppgift, vilket innebär att bolaget först i efterhand kommer att kunna nyttja uppförandekodens regelverk.

3.3. **Utbildning**

Marknadschefen som driver GDPR-arbetet inom bolaget har deltagit vid ett utbildningstillfälle som SABO[3] arrangerade i januari månad 2018 och hen har även genomfört en webbutbildning om dataskyddsförordningen.

För kontorspersonalen har ett utbildningspass på en timme genomförts under februari. VD och ledningsgrupp har fått fortlöpande information, dock ännu inte i form av regelrätt utbildning. Styrelsen informerades om förordningen vid sammanträdet den 6 mars.

Uppfattningen är att det säkerligen behövs genomföras fler utbildningstillfällen och att bolaget troligtvis kan komma att behöva en extern föreläsare. Detta är dock något som bolaget planerar att ta ställning till efter att förordningen har trätt ikraft.

[3] Sveriges allmännyttiga bostadsföretag

Building a better working world

4. Bedömning

Vår sammanfattande bedömning är att styrelsen arbetar på ett ändamålsenligt sätt med planering och anpassningar inför införandet av den nya dataskyddsförordningen. Vi kan konstatera att arbetet med att identifiera nödvändiga förändringar med anledning av införandet av förordningen har påbörjats. Det saknas dock dokumentation kring bolagets slutsatser. Däremot har en tidplan med åtgärderna som ska vidtas och som redogör för att åtgärderna kommer att hinna genomföras i tid inför ikraftträdandet upprättats.

Vi noterar att bolaget planerar att upprätta register över vilka behandlingar av personuppgifter som sker i bolagets olika processer samt samla dessa i ett gemensamt dokument. Då bolagets GDPR-arbete i planeringsfasen är bedömningen att det ännu inte finns aktuella och ändamålsenliga rutinbeskrivningar för hur personuppgifter ska hanteras. Enligt tidplanen ska dessa vara på plats inför förordningens ikraftträdande.

Vi har även noterat att styrelsen har utsett ett dataskyddsombud som ska anmälas till Datainspektionen. Det är av vikt att påminna om dataskyddsombudets självständighet och oberoende. Dataskyddsombudet ska inte ha andra arbetsuppgifter som kan krocka med rollen som dataskyddsombud. Exempelvis anses det inte vara lämpligt att dataskyddsombudet sitter i organisationens ledning eller är med och fattar strategiska beslut om kärnverksamheten som omfattar personuppgiftsbehandling.

En av riskerna som vi ser är att bolaget inte har tagit höjd för att det kan finnas fler leverantörer som de måste upprätta personuppgiftsbiträdesavtal med då de inte har genomfört en mer djupgående analys. Vi anser även att det kommer att krävas ytterligare utbildningstillfällen för medarbetarna och att det är av vikt att styrelsen säkerställer att det kommer att ske innan lagens ikraftträdande.

Revisionsfrågor	Svar
Har styrelsen tydliggjort ansvaret?	Delvis, de har uppdragit VD att genomföra nödvändiga anpassningar. VD har utsett marknadschefen till bolagets dataskyddsombud.
Har nödvändiga förändringar med anledning av införande av förordningen identifierats?	Delvis, det framgår av intervjun att de har påbörjat arbetet med att identifiera nödvändiga förändringar. Det kan finnas risker med att bolagets samtliga leverantörer inte är identifierade då det inte har gjorts en heltäckande analys. Däremot har en tidplan upprättats som anger när de identifierade åtgärderna ska genomföras.
Har nödvändiga anpassningar påbörjats i rimlig omfattning?	Nej, åtgärderna har identifierats och kontakter med leverantörer är vidtagna. Dock har inte det praktiska arbetet påbörjats. Enligt tidplanen ska bolaget tillsätta arbetsgrupper som ska genomföra arbetet under april 2018.
Finns aktuella och ändamålsenliga rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheterna?	Delvis. Vi har tagit del av är ett utkast på dokumentet Register för intresseanmälan samt en rapport för personuppgiftsincidenter.

Har nyckelpersoner i bolagen informerats om förändringarna och dess innebörd på ett tillräckligt sätt?	Nej, främst kortare informationstillfällen eller utbildningspass men i sammanhanget kan det inte anses vara tillräckligt.

Utifrån granskningsresultatet rekommenderar vi styrelsen att:

- genomföra en mer omfattande analys av nödvändiga anpassningar samt dokumentera slutsatserna,
- säkerställa att det finns tillräckliga rutinbeskrivningar för hur personuppgifter ska hanteras i verksamheten, samt
- säkerställa att personalen informeras i tillräcklig utsträckning inför ikraftträdandet.

Kävlinge den 23 april 2018

Negin Nazari
EY

Sara Shamekhi
EY

Building a better working world

***Bilaga 1:* Källförteckning**

Intervjuade funktioner:

- Eva Hansson marknadschef

Medverkat vid intervjuerna:

- Fernando Dinis Viseu, förtroendevald revisor
- Dietmar Olbrich, förtroendevald revisor

Dokument:

- GDPR – handlingsplan KKB
- Register för intresseanmälan
- Rapport – personuppgiftsincident
- Tidplan
- Protokoll