Kristianstads kommun

KOMMUNREVISIONEN

2020-01-06

Kristianstads kommun
Styrelsen för ABK

För kännedom till:
Kommunstyrelsen
Kommunfullmäktige

Arbetet med införande av GDPR- Förstudie avseende ABK

Kristianstads kommuns lekmannarevisorer har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskydds-förordningen (GDPR) genomförts i det kommunala bostadsbolaget ABK och därvid bilda sig en uppfattning om nuläget.

Frågeställningen för denna förstudie är således: *"Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?".*

Efter genomförd förstudie får frågeställningen besvaras med ett ja. Bolaget har generellt sett tagit ett helhetsgrepp på frågorna kring skyddet av personuppgifter och har ett behandlingsregister på plats. Kontrollen är generellt sett god inom organisationen (baserat på den översiktliga studie som här genomförts) och åtgärder har vidtagits för att säkerställa att kunskap kring personuppgiftsbehandling kommer på plats, exempelvis genom utbildningar. Nivån enligt applicerad frågemetodik ger ett resultat som ligger över, och ibland mycket över, den grundläggande nivån.

Mot bakgrund av vad som framkommit i vår förstudie vill vi lyfta fram följade rekommendationer:

- Dokumentera oberoendeanalysen kring nuvarande dataskyddsombud.
- Tillse att utpekad roll som dataskyddsombud är oberoende gentemot bl.a. ledningsgrupp och kan utföra de granskningar av efterlevnaden på området som ingår i uppdraget.
- Dokumentera rättslig grund i behandlingsregistret ("Gallringsrutiner").
- Överväg att införa riktlinjer som särskilt hanterar frågan om ostrukturerad data.

För lekmannarevisorerna i Kristianstads kommun

Sven Gunnar Linné
Ordförande

Göran Sevebrant
Vice ordförande

Arbetet med införandet av GDPR inom ABK - en förstudie och nulägesbeskrivning

Linus Owman

Peter Olby

pwc

Innehåll

1. Inledning

1.1 Bakgrund - GDPR

EU:s dataskyddsförordning, General Data Protection Regulation (GDPR), innebär en skärpning av dataskyddslagstiftningen inom EU, både avseende organisationers åligganden och de registrerade personernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare. För att den ska respekteras införs möjligheten till kraftfulla sanktioner för de organisationer som ignorerar eller brister i att uppfylla de nya kraven. Sanktionsnivåerna har valts så att de ska vara avskräckande och för att det inte ska löna sig att bryta mot reglerna för att spara pengar. Väsentliga sanktionsavgifter för bristande efterlevnad, upp till 20 miljoner kronor, kan utfärdas för myndigheter. Det införs också en rätt för privatpersoner att kräva skadestånd av de organisationer som inte tillhandahåller deras rättigheter enligt förordningen. Förordningen började tillämpas den 25 maj 2018.

Förordningen innehåller nya krav jämfört med Personuppgiftslagen, som exempelvis att alla organisationer själva har en skyldighet att bedöma riskerna för att de registrerades integritet kränks samt vidta lämpliga åtgärder för att minska dessa risker. Organisationer måste även i vissa fall utse dataskyddsombud och rapportera allvarliga personuppgifts incidenter till tillsynsmyndigheten (och i vissa fall de berörda registrerade) inom 72 timmar. Om man misstänker att någon personuppgiftsbehandling kan medföra höga integritetsrisker för de registrerade måste man göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador. Revisorerna har i sin riskbedömning lyft fram att det är väsentligt att genomföra en förstudie för att bilda sig en initial uppfattning om status för området. Förstudien ingår i revisionsplanen för år 2019.

1.2 Syfte och frågeställning

Kristianstads kommuns lekmannarevisorer har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts i det kommunala bostadsbolaget ABK och därvid bilda sig en uppfattning om nuläget.

Frågeställningen för denna förstudie är således: *“Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?”.*

Frågeställningen ovan har besvarats genom ett intervjuformulär. Intervju har genomförts i gruppform tillsammans med bolagets dataskyddsombud, IT-chef, samt bolagets externa juridiska rådgivare. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter

- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

1.3 Avgränsning och metod

Förstudien syftar inte till att kartlägga *de facto* efterlevnad av direktivet, då detta skulle ha mer av en granskande karaktär, dvs falla utanför ansatsen hos en förstudie. Förstudien har därför i sin ansats fokuserat på att ge en generell bild av hur arbetet genomförts och fortskrider, utan att detaljerade studier genomförts på förvaltningsnivå. Översiktliga dokumentstudier har genomförts.

Intervju har således genomförts med personer som representerar de funktioner med ett särskilt ansvar i införandet av GDPR.

2. Kartläggning

2.1 Bakgrund - införandet av GDPR

Liksom för andra organisationer innebar 2018 bråda dagar i termer av införandet av den nya dataskyddsförordningen. Arbetet initierades av den juridiska avdelningen under 2017, för att sedan intensifieras. Bolaget har ett utsett dataskyddsombud (DSO), vilket är samma person som även är ledningsrepresentant och ansvarig för verksamhetsgrenarna bygg och lokaler. DSO började sin bana inom bolaget som företagsjurist och anses av bolaget därmed ha den bakgrundsexpertis som bolagsledningen uppfattade behövdes för införandet av GDPR. DSO har haft ytterligare stöd i införandet av GDPR i de stödfunktioner som den juridiska avdelningen har (en person), samt i den externa bolagsjurist (Glimstedt) som regelbundet anlitas av ABK.

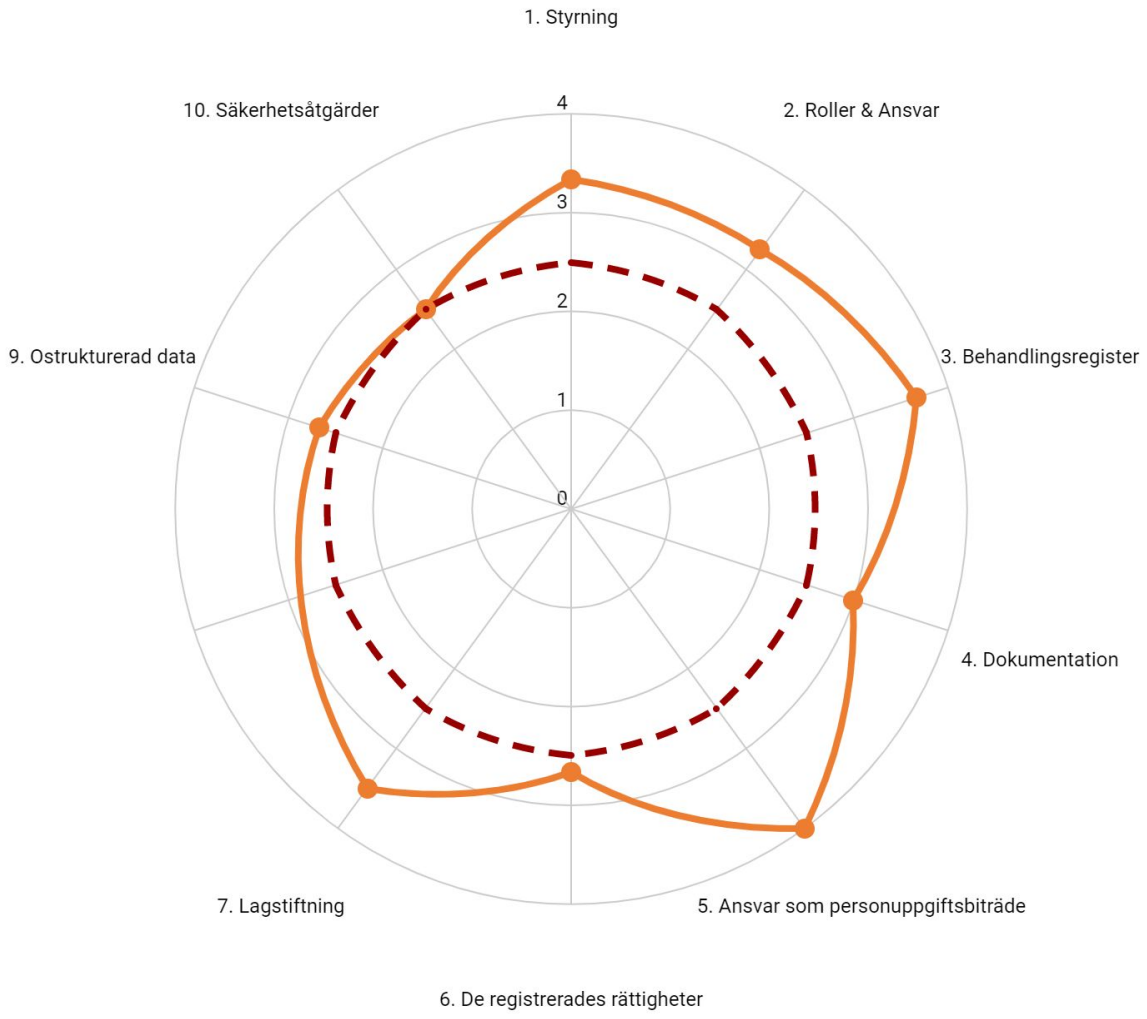
För att hantera införandet bildades en projektgrupp bestående av bolagsjurist (senare DSO), IT-chef, samt det externa juridiska stödet. Projektgruppen avrapporterade regelbundet till bolagets styrelse.

2.2 Övergripande resultat

För att sammanställa denna rapport har PwC intervjuat relevanta personer med insyn i ABKs dataskyddsarbete och det anpassningsarbete som gjorts till GDPR.

Diagrammet nedan visar resultatet av vår genomgång. Diagrammet är baserat på intervjusvar till 35 standardiserade frågor och ger en översiktsbild av alla relevanta områden för korrekt hantering av personuppgifter.

Den orangea linjen representerar ABKs resultat. Den röda prickade linjen utgör grundvärde för vad vi bedömer är ett godkänt dataskyddsarbete. Medelvärdet för detta är 2,5. Värdet är baserat på en generell bedömning utifrån intervjuformulärets svarsalternativ. Alternativ 1,0 innebär att bolaget inte påbörjat något arbete alls inom området och alternativ 4,0 innebär i korthet att bolaget infört en fullständig (och ofta automatiserad) process kring behandlingen. Ett värde på 2,5 innebär således att organisationen ligger över både 1,0 (inget gjort) och 2,0 (lite gjort) och tangerar 3,0 (vidtagit åtgärder). Ett område (nr. 8 “Barn”, har utgått, se avsnitt 3.8).



Den sammanfattande bedömningen är att ABK har gjort ett gediget arbete i att ta sig an de utmaningar som den nya dataskyddsförordningen innebär. Bolaget ligger konsekvent över den nivå som vi betraktar som grundnivå. I vissa delar ligger bolaget nära den högsta möjliga nivån, baserat på den översiktliga studie som genomförts.

I den fortsatta rapporten går vi djupare in på varje område och ger specifika rekommendationer.

3. Resultat

3.1 Styrning

Bolagets resultat för området är **3,3 av 4,0**. Det har funnits ett tydligt uppdrag att införa GDPR. Arbetet initierades av den juridiska avdelningen under 2017, för att sedan intensifieras. Bolaget har ett utsett dataskyddsombud (DSO), vilket är samma person som även är ledningsrepresentant och ansvarig för verksamhetsgrenarna bygg och lokaler. DSO började sin bana inom bolaget som företagsjurist och anses av bolaget därmed ha den bakgrundsexpertis som bolagsledningen uppfattade behövdes för införandet av GDPR. DSO har haft ytterligare stöd i införandet av GDPR i de stödfunktioner som den juridiska avdelningen har (en person), samt i den externa bolagsjurist (Glimstedt) som regelbundet anlitas av ABK.

För att hantera införandet bildades en projektgrupp bestående av bolagsjurist (senare DSO), IT-chef, samt det externa juridiska stödet. Projektgruppen avrapporterade regelbundet till bolagets styrelse. Då nuvarande DSO även sitter med i ledningsgruppen får projektgruppen anses ha haft det mandat som krävs för att införa GDPR. Det som drar ner poängen inom detta område är avsaknaden av en strukturerat arbete med informationsklassning inom bolaget.

3.2 Roller och ansvar

Inom området roller och ansvar har bolaget erhållit resultatet **3,3 av 4,0**. Bolaget har en utpekad roll för dataskyddsombud, och ett sådant är tillsatt. När det gäller det allmänna arbetet med informationssäkerhet finns i nuläget ingen utpekad roll med detta ansvar, vilket drar ner poängen något.

Avseende rollen som DSO är det inte säkert att bolaget i formell mening behöver en sådan funktion eftersom bolaget har färre än 250 anställda. Inte desto mindre har bolaget valt att formellt utse ett sådant och är då enligt förordningen skyldiga att löpan linan ut ifråga om rollens beskaffenhet. Här bör det även påpekas att rollen som dataskyddsombud bör betraktas som något liknande en internrevisor, vilket innebär att personen behöver vara oberoende. En oberoendeanalys genomfördes innan rollen som DSO tillsattes, men analysen dokumenterades inte. För att i någon mån säkra oberoendet har extern juridisk hjälp regelbundet inkallats till stöd i bl.a. arbetet med GDPR. Detta är dock inte en roll som kan ikläda sig ansvaret som DSO.

Det finns planer på att adressera oberoendet genom intern kontroll och granskning var 3:e år. Detta är emellertid inte dokumenterat.

Rekommendation:

- Dokumentera oberoendeanalysen kring nuvarande DSO.
- Dokumentera planer på att säkerställa oberoendet genom granskning av intern kontroll, och hur ofta detta bör ske.

- Tillse att utpekad roll som dataskyddsombud är oberoende gentemot bl.a. ledningsgrupp och kan utföra de granskningar av efterlevnaden på området som ingår i uppdraget.

- Utpeka ansvar för informationssäkerhet i organisationen.

3.3 Behandlingsregister

För detta område har bolaget erhållit ett resultat på **3,7 av 4,0**. Bolaget har gjort en kartläggning av sina behandlingar av personuppgifter. Detta återfinns i två huvudsakliga dokument (“System- och personuppgiftsförteckning” samt “Gallringsrutiner”). System- och personuppgiftsbeteckningen ger ingen helhetsbild av alla de personuppgiftsbehandlingar som sker inom respektive system, eftersom registret tar sin utgångspunkt i respektive system och det faktum att behandlingar sker i respektive system. Vilka behandlingar som sker framgår inte. Dokumentet “gallringsrutiner” är mer ändamålsenligt utifrån personuppgiftsbehandlingar, eftersom det för varje system bl.a. innehåller såväl den enskilda behandlingen som ändamål och tidsbegränsning. Dock saknas dokumenterad rättslig grund.

Bolaget har en förteckning över behandlingar som sker hos tredje part (“Förteckning över PUB-avtal”). Inga behandlingar sker utanför EU/EES.

Rekommendation:

- Dokumentera rättslig grund i behandlingsregistret (“Gallringsrutiner”).

- Överväg att kalla dokumentet “behandlingsregister för personuppgifter” eller liknande, så att det råder klarhet kring vilket dokument som utgör behandlingsregister.

- Överväg att sammanföra innehållet i dokumenten “System- och personuppgiftsförteckning” samt “Gallringsrutiner” till ett enhetligt behandlingsregister.

3.4 Dokumentation

Inom frågeområdet för dokumentation ligger bolaget på **3,0 av 4,0**. Bolaget har en integritetspolicy och tydlig information på hemsidan kring hur behandlingen av personuppgifter går till och till vem den registrerade kan vända sig med frågor, även om det inte i alla delar framgår exakt vilka behandlingar som utförs. Det finns även en mall för personuppgiftsbiträdesavtal att tillgå. Policyn är undertecknad av VD samt DSO.

Utöver detta finns en IT-policy vilken är under omarbetning med avseende på GDPR, samt en policy kring utlämnande av allmänna handlingar.

Det som saknas är riktlinjer som på ett mer vägledande sätt bryter ner policyns viljeyttring till konkreta åtgärder som implementeras på varje nivå, eller på varje specifik enhet i organisationen. En annan iakttagelse är att det inte är lämpligt att DSO, i kraft av sitt oberoende, skriver under en policy tillsammans med VD.

Rekommendation:

- Säkerställ att riktlinjer och/eller rutiner på mer detaljerad nivå än integritetspolicyn styr hanteringen av personuppgifter ute i organisationen.

- Överväg att inte ha DSO som undertecknad på integritetspolicyn.

3.5 Ansvar som personuppgiftsbiträde

Bolaget hamnar här på **4,0 av 4,0**. Bolaget agerar sällan personuppgiftsbiträde till andra verksamheter, men har identifierat de tillfällen då detta sker. Det finns även mallar för personuppgiftsbiträdesavtal.

I enstaka fall har leverantörer krävt att bolaget ska underteckna deras PUB-avtal, vilket i praktiken innebär att ABK då ikläder sig rollen som personuppgiftsbiträde.

3.6 De registrerades rättigheter

För frågeområdet kring de registrerades rättigheter hamnar bolaget på **2,7 av 4,0**. Bolaget har via hemsidan rutiner för att upplysa den registrerade om hur personuppgifter behandlas. Informationen kommuniceras även till hyresgäster via mail och månadsblad.

Det finns ingen dokumenterad process för hur registerutdrag lämnas ut, hur rättning eller radering av felaktiga personuppgifter sker. Bolaget tillämpar inte automatiskt beslutsfattande, men det saknas möjlighet för den registrerade att invända som viss behandling av personuppgifter.

Avseende personal raderas alla personer som avslutar sin anställning på ABK, utom i de delar som krävs för att fullgöra bolagets skyldigheter inom annan tillämplig lagstiftning, exempelvis arkivlagen.

Rekommendation:

- Överväg att dokumentera processerna för hur de registrerades rättigheter ska tillgodoses när en formell begäran inkommer, oaktat vilken rättighet som åberopas.

3.7 Lagstiftning

Avseende bevakning av lagstiftningsområdet inom dataskyddsområdet har bolaget en utpekad funktion kring detta (dvs bolagsjuristen och i förekommande fall dataskyddsombudet, samt externt juridiskt stöd). Bolaget hamnar här på **3,5 av 4,0**.

3.8 Barn

Bolaget behandlar inte personuppgifter för barn där föräldrarnas samtycke behöver inhämtas. Givet att bolaget inte behandlar personuppgifter för barn har frågan utgått.

3.9 Ostrukturerad data

Avseende området ostrukturerad data är resultatet att bolaget ligger på **2,7 av 4,0**.

Det behandlingsregister som bolaget upprättat väger inte in ostrukturerad data. Personalen har informerats om hur de ska göra för att minimera användningen av ostrukturerad data, men det saknas riktlinjer för hur detta ska ske praktiskt. Det blir därmed svårt att följa upp arbetet och bolaget säger sig inte heller ha full kontroll på efterlevnaden av detta. Personalen har delvis utbildats i förhållandet till ostrukturerad data.

Rekommendation:

- Säkerställ efterlevnaden kring lagring av data på godkända fildelningsytor. Överväg hård- och mjukvaruspärrar för att förhindra lagring på otillåtna sätt, exempelvis genom spärr för USB-minnen, installation av Dropbox etc.

- Överväg att införa riktlinjer som särskilt hanterar frågan om ostrukturerad data.

3.10 Säkerhetsåtgärder

Inom området säkerhetsåtgärder får bolaget **2,5 av 4,0**.

Avseende utvecklingen av verksamhetssystemet Vitec har bolaget haft löpande dialog med utvecklarna kring att minimera fritext och möjliggöra effektiv gallring.

Bolaget har genomfört flera generella och fördjupade utbildningar och informationstillfällen där bestämmelserna kring personuppgifter varit i fokus, beroende på åhörargrupp. Det finns möjligheter att lägga in uppgifter om om vem som genomgått vilken typ av utbildning och vid vilket tillfälle genom registrering i personalsystemet. Då bolaget har har relativt hög personalomsättning är detta ett kontinuerligt arbete.

Det finns i nuläget ingen dokumenterad process för att genomföra konsekvensbedömningar kopplat till personuppgiftsbehandlingar som bedöms utgöra hög risk för den registrerade.

Avseende personuppgiftsincidenter finns det rutiner kring att DSO ska kontaktas men processen kring hur detta sedan sker är inte fullt ut dokumenterad.

Rekommendation:

- Säkerställ att incidenthanteringsrutiner är på plats och övade inom hela organisationen. En incident är aldrig fråga om *om* utan om *när*. Rutiner kring incidenthantering bör vara kända i alla delar av organisationen. Denna medvetandehöjande insats kan med fördel kombineras med utbildning kring ostrukturerad data (se 3.9 ovan).

- Säkerställ att processen för konsekvensbedömningar dokumenteras och tillämpas, exempelvis genom övningar på mindre känsliga case för att bygga en vana kring detta inom organisationen.

4. Slutsatser

Inledningsvis ställdes frågan *"Har ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna?"* Frågeställningen har besvarats genom ett intervjuformulär som besvarats genom intervjumetodik. Intervjuer har genomförts i gruppform och de flesta av bolagets förvaltningar har därvid varit representerade. Områdena som täckts in genom intervjuerna har varit:

- Styrning
- Roller och ansvar
- Register över behandlingar av personuppgifter
- Dokumentation
- Ansvar som personuppgiftsbiträde
- De registrerades rättigheter
- Lagstiftning
- Barn
- Ostrukturerad data
- Säkerhetsåtgärder

Svaret på frågeställningen om huruvida "*ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna"* får besvaras med ett ja.

Bolaget har generellt sett tagit ett helhetsgrepp på frågorna kring skyddet av personuppgifter och har ett behandlingsregister på plats. Kontrollen är generellt sett god inom organisationen (baserat på den översiktliga studie som här genomförts) och åtgärder har vidtagits för att säkerställa att kunskap kring personuppgiftsbehandling kommer på plats, exempelvis genom utbildningar.

Nivån enligt applicerad frågemetodik ger ett resultat som ligger över, och ibland mycket över, den grundläggande nivån. Liksom inom andra områden finns det alltid utrymme för förbättringar och ett fåtal rekommendationer har föreslagits i föregående avsnitt.

Det tydligaste förbättringsområden för bolaget avseende frånvaron av konkreta riktlinjer för olika områden inom behandling av personuppgifter. Den nuvarande integritetspolicyn är allmänt hållen och tydligare riktlinjer avseende hur hur de registrerades rättigheter tillgodoses och hur övriga personuppgiftsbehandlingar bör ske ute i organisationen bör komma på plats.

Bolaget skulle vidare vara betjänt av att koppla arbetet med skyddet av personuppgifter till ett bredare informationssäkerhetsarbete, med åtföljande IT-styrning kring exempelvis hård- och mjukvara, för att säkerställa att policyer och rutiner även får genomslag i konfiguration av system, applikationer och hårdvara. På så sätt minskas risken för mänskliga oavsiktliga fel och antagonistiska handhavanden med avsikt att skada.

“Dataskyddsförordningen (The General Data Protection Regulation) är till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.”

Datainspektionens hemsida