Kristianstads kommun

KOMMUNREVISIONEN

2021-05-19

Styrelsen för Kristianstad Renhållning AB
Kommunstyrelsen för kännedom

Förstudie och nulägesbeskrivning arbetet med införandet av GDPR

PwC har på uppdrag av de förtroendevalda revisorerna i Kristianstads kommun genomfört en förstudie avseende införandet av GDPR inom KRAB. Förstudiens syfte har varit att bedöma om ett ändamålsenligt och heltäckande arbete gällande GDPR har bedrivits och om åtgärder har vidtagits för att efterleva de nya reglerna.

KRAB bedriver ett ändamålsenligt och heltäckande arbete gällande GDPR åtgärder har vidtagits för att efterleva de nya reglerna. Organisationen ligger i flera fall över den grundnivå som kan anses vara acceptabel vid införandet av GDPR, men får trots detta sägas ha förbättringspotential inom ett antal områden. Därför har, trots det grafiskt goda resultatet, ett 20-tal rekommendationer föreslagits i rapporten, se bifogad bilaga.

Renhållningen har en generell medvetenhet gällande GDPR och arbetar med att skydda personuppgifter på ett bra sätt. Bolaget har stöd från kommunens jurister i frågor kring dataskydd och andra regulatoriska frågor, liksom ifråga om användning av PUB-avtal. Bolaget använder sig av samma dataskyddsombud som Kristianstad kommun (JP Infonet). Bolaget har vidtagit åtgärder och utbildat personal, men roller och ansvar kring dataskydd och informationssäkerhet är fortfarande inte fullt ut definierade i organisationen. Renhållningen har en tydlig registerförteckning och en systemförteckning på plats som tydligt beskriver organisationens behandlingar kopplat till system. Däremot ser vi att systemförteckningen och registerförteckningen inte helt stämmer överens med varandra, vilket innebär att det förekommer behandlingar av personuppgifter som inte ännu förts in i registerförteckningen.

Granskningsrapporten överlämnas till Kristianstad Renhållnings styrelse för besvarande senast den 30 september år 2021 och till kommunstyrelsen för kännedom. Svar skickas till revisionen@kristianstad.se och till det sakkunniga biträdet lena.salomon@pwc.com

För revisorerna i Kristianstads kommun

Sven Gunnar Linné
Ordförande

Göran Sevebrant
Vice ordförande

Arbetet med införandet av GDPR, KRAB - en förstudie och nulägesbeskrivning

Linus Owman

Omid Asali

Simon Sundberg

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 åtaganden och de registrerade individernas rättigheter. Den gäller för alla organisationer, företag och myndigheter som hanterar uppgifter om EU-medborgare. För att den ska respekteras infördes 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 infördes 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, genom SFS 2018:218 Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (även benämnd dataskyddslagen i dagligt tal).

Lagen 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 personuppgiftsincidenter till tillsynsmyndigheten (och i vissa fall de berörda registrerade) inom 72 timmar. Om organisationen misstänker att någon personuppgiftsbehandling kan medföra höga integritetsrisker för de registrerade måste organisationen göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador.

I slutet av juni 2020 publicerade tidningen “Aktuell Säkerhet” en debattartikel kring införandet av GDPR och aktuellt läge. Några korta citat hjälper till att belysa denna förstudies aktualitet ytterligare:

“Efter en förhållandevis lugn start slogs det i mars i år rekord i antal utfärdade böter inom ramarna för GDPR. Idag, när digitaliseringen ute på företagen går ännu snabbare i svallvågorna av den globala pandemin är det absolut nödvändigt att företag inte bara förstår det ansvar de har över sina kunders data, utan att de i samma snabba takt utvecklar sitt dataskydd och säkerhetsarbete. .../…// För små och medelstora företag är de potentiella konsekvenserna svårare att överblicka. De har i regel stramare budgetar och mindre IT-avdelningar och riskerar att bli överväldigade av de resurser och de insatser som krävs för ett fullgott dataskydd. Att samtidigt säkerställa efterlevnad av GDPR gör situationen än mer komplicerad. Det finns gott om åtgärder som kan vidtas utan stor budget. Att investera i lösningar för dataskydd och strategier är en grundläggande del i att framtidssäkra en verksamhet i en digital värld. Kort sagt – dataskydd behöver vara en central del i verksamhetens affärsstrategi – inte minst i takt med att IT-sidan blir alltmer komplex.” [1]

[1] https://www.aktuellsakerhet.se/gdpr-fyller-tva-hur-har-det-gatt/

1.2 Syfte och frågeställning

Kristianstad kommuns revisorer har uppdragit åt PwC att genomföra en förstudie kring hur arbetet med införandet av bestämmelserna kopplade till den nya dataskyddsförordningen (GDPR) genomförts inom det kommunägda bolaget Kristianstad Renhållnings AB och därvid bilda sig en uppfattning om nuläget. Förstudien ingår i revisionsplanen för år 2021.

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 en gruppintervju. 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 fokuserat på att ge en generell bild av hur arbetet genomförts och fortskrider. Översiktliga dokumentstudier har genomförts.

Intervju har således genomförts med personer som representerar de funktioner med ett särskilt ansvar i införandet av GDPR. Intervju har genomförts i gruppform tillsammans med VD Johan Karlsvärd, Operativ chef Christian Edwardsson, Administrationschef Ann Sventorp, Ekonomiassistent Isabell Giuffrida och IT-förvaltare Peter Aronsson.

2. Kartläggning

2.1 Bakgrund - införandet av GDPR

Arbetet med införandet av GDPR inom Kristianstad Renhållnings AB (härefter: Renhållningen) initierades i samband med att lagstiftningen trädde i kraft 2018. Tidigare hade Renhållningen förhållit sig till förut gällande PuL-lagstiftning. Renhållningen har enligt egen utsaga prioriterat arbetet med GDPR efter bästa förmåga och organisatorisk kapacitet. I arbetet har Renhållningen haft stöd från Kristianstad kommun i form av anpassning till dataskyddsförordningen, samt som stöd vid frågor, och arbetet har därmed kunnat genomföras med effektivitet. Kommunen har haft vissa utmaningar med befattningen av dataskyddsombud och har sedan en tid tillbaka landat i en lösning med ett externt dataskyddsombud (JP Infonet), vilket också är det dataskyddsombud som Renhållningen har att tillgå.

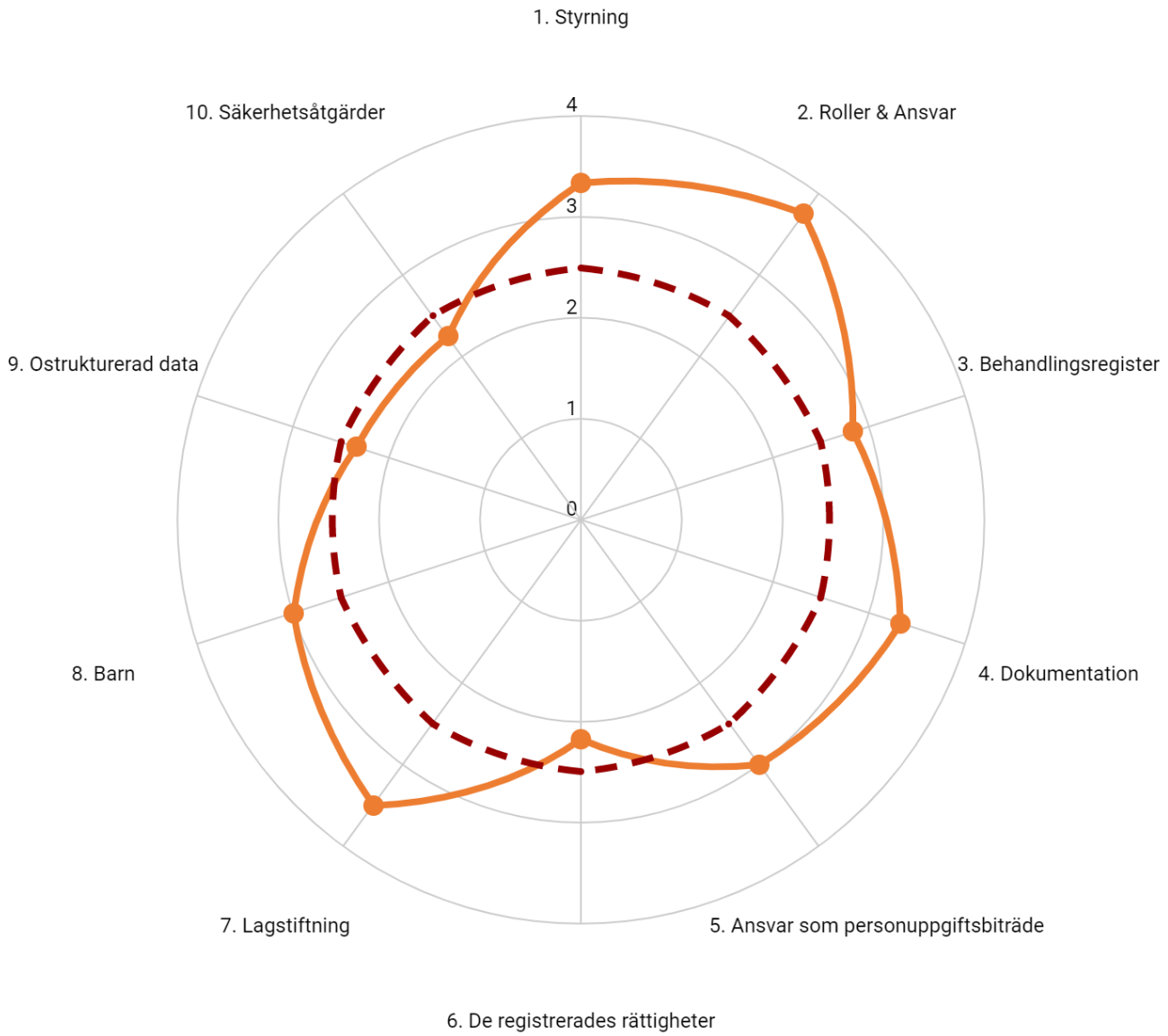
Renhållningen har gått igenom de system som bolaget har och granskat de uppgifter som behandlas rent säkerhetsmässigt. Arbetet har genomförts stegvis och bolaget har prioriterat de system som anses viktiga och tagit stöd från kommunen i den mån det behövts.

2.2 Övergripande resultat

För att sammanställa denna rapport har PwC intervjuat relevanta personer med insyn i Renhållningens 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 Renhållningens 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 Renhållningen inte påbörjat något arbete alls inom området och alternativ 4,0 innebär i korthet att Renhållningen infört en fullständig (och ofta automatiserad) process kring behandling. 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).



Den sammanfattande bedömningen är att Kristianstad Renhållnings AB i flera väsentliga delar vidtagit åtgärder för att uppnå regelefterlevnad i enlighet med GDPR, och bolaget ligger i flera delar över det vi betraktar som en grundnivå. Ett område som sticker ut negativt är område 6, de registrerades rättigheter, där bolaget har kvarstående förbättringsåtgärder. Området är särskilt viktigt eftersom det är just datasubjektens rättigheter som lagstiftningen syftar till att värna. I den fortsatta rapporten går vi djupare in på varje område och ger specifika rekommendationer.

3. Resultat

3.1 Styrning

Bolagets resultat för detta område är **3,3 av 4,0**. Det har funnits en tydlig ambition med uppdrag från ledningsgruppen, ut i organisationen, att införa GDPR. Arbetet har främst drivits framåt av VD, IT-förvaltare och Ekonomiassistent med stöttning från kommunens jurister för att kontrollera så att införandet går i rätt riktning.

Renhållningen är uppmärksammad på att hantering av personuppgifter berör hela organisationen då GDPR är i fokus. Bolaget har således påbörjat ett arbete med att anpassa sig till den lagstiftning som finns och har i arbetet tagit spjärn mot sina erfarenheter av regelefterlevnad gentemot PuL (personuppgiftslagen).

Bolaget är medvetet om vad som krävs för att uppnå regelefterlevnad enligt GDPR, men det råder ibland delade meningar inom verksamheten om vad som skall gälla. I dagsläget är det Renhållningens IT-förvaltare och Ekonomiassistent som arbetar med frågor kring dataskydd och ökad mognad inom bolaget, med kommunens jurister som extra stöd om det behövs.

All digital informationstillgång styrs via behörigheter och fysiska dokument förvaras i skåp som utvalda medarbetare har tillgång till. I nuläget är Renhållningen inte medvetna om det finns en förmåga att klassificera dokument från ett tekniskt perspektiv men i dokumentet *Digital kommunikation* (2015, reviderat 2017) beskrivs hur bolagets information ska klassificeras i gemensamma stödsystem och egna register/ dokument. Enligt dokumentet ska detta göras för att nå en säker informationshantering och klassning ska ske utifrån sekretess, tillgänglighet, riktighet, spårbarhet. Klassningen ska genomföras avseende all information, där möjlighet till lagring finns. Enligt dokumentet sker informationsklassning av all information, oavsett hur informationen finns lagrad. Klassificeringen av informationen är dock inte fullt ut genomförd, och det sker inte en konsekvent klassning mellan känslig information och övrig information. Vidare kan konstateras att dokumentet inte blivit uppdaterat sedan 2017 och att dokumentet hänvisar till personuppgiftslagen (PuL).

Rekommendationer:

- *Säkerställ att den informationsklassificering som genomförs även tar sig uttryck i tekniska kontroller på systemnivå.*
- *Uppdatera dokumentet "Digital kommunikation" så att det avspeglar kraven som ställs på organisationen utifrån GDPR.*
- *Säkerställ att det görs en tydlig skillnad mellan känsligt och icke känsligt material.*

3.2 Roller och ansvar

Inom området roller och ansvar har Renhållningen erhållit resultatet **3,8 av 4,0**. Renhållningen har utvärderat om ett eget dataskyddsombud är nödvändigt och landat i ett besult att inte tillämpa en sådan roll för bolaget. Renhållningen har istället beslutat att använda sig av Kristianstad kommuns dataskyddsombud. Kommunen använder JP Infonet som extern leverantör. Vidare har Renhållningen hittills inte utnyttjat detta stöd från Kristianstads kommun.

Ansvaret för Renhållningens informationssäkerhet finns implicit definierat i *Digital kommunikation*, men inga tydliga roller är definierade och ansvaret är således inte fullt ut dokumenterat i organisationen. Bolaget har även identifierat vilka enheter inom bolaget som hanterar olika typer av personuppgifter och som ansvarar för specifika personuppgiftsbehandlingar. I dagsläget är det Renhållningens IT-förvaltare och Ekonomiassistent som arbetar med frågor kring regelefterlevnad, dataskydd och ökad mognad inom bolaget, med kommunens resurser som extra stöd om det efterfrågas.

Granskning av efterlevnad sker kontinuerligt och korrigeringar sker så fort som möjligt. Med tanke på organisationens storlek görs enligt de intervjuade interna kontroller för att mäta prestationen och identifiering av punkter där potentiella förbättringar finns.

Information om vad som bedöms och definieras som en personuppgift kommuniceras ut i organisationen av IT-förvaltaren. För information och ökad mognad kring dessa frågor brukar bolaget i vanliga fall ha fysiska utbildningar för dem som det berör, något som fått stå tillbaka under pandemin. Bolagets bedömning är att det i nuläget är oklart om alla vet vad som definieras som en personuppgift in i minsta detalj, men att alla anställda samtidigt har en grundläggande förståelse.

Rekommendationer:

- *Förtydliga roller och ansvar för informationssäkerhet i relevant dokumentation, exempelvis i dokumentet Digital kommunikation, IT-policy etc.*

3.3 Behandlingsregister (registerförteckning)

För detta område har bolaget erhållit ett resultat på **2,8 av 4,0**.

Renhållningen använder verktyget EDP-future som kunddataregister och från detta extraheras ett underlag som delvis ligger till grund för organisationens registerförteckning, vilket utgörs av en Excel-fil. I denna fil är det tydligt definierat för vilka syften som Renhållningen behandlar personuppgifter för att utföra det arbete som krävs, exempelvis hämtning och fakturering på de kunder som finns registrerade, samt löner till anställda. Registerförteckningen behandlar vidare löpnummer, kategorier, vilka system, vilka personer behandlingen omfattar etc. I jämförelsen mellan vilka uppgifter som finns i EDP future samt i registerförteckningen finns dock viss diskrepans, vilket gör att ett fullständig bild av alla de behandlingar som bolaget genomför framträder först genom en kombination av både EDP future och dokumentet registerförteckning.

Under intervjuer framhåller bolaget att de inte överför personuppgifter mellan organisationen och leverantörer (exempelvis entreprenörer), men organisationen har inte kartlagt vilka

överföringar som sker till mottagare utanför organisationen, exempelvis till kommunen. Detta framgår bland annat av att “kolumn I” i registerförteckningen inte är ifylld. Renhållningen anser sig dock ha en tydlig bild om varför och vilka personuppgifter som skickas över.

Renhållningen har inte varit med om att personuppgifter har förts över till mottagare utanför EU/ EES, men det skulle kunna ske exempelvis via e-post. Samtidigt visar systemförteckningen att organisationen använder en rad molnbaserade lösningar, där bolaget inte tydligt säkerställt informationens geografiska hemvist. Renhållningen använder exempelvis VISMA som sitt personal- och driftsystem. Här vet organisationen inte säkert var deras servrar finns och var informationen hanteras och lagras, något som lagstiftningen kräver avseende att säkerställa att informationen inte lämnar EU/EES-området.

När det gäller radering och gallring av personuppgifter hänvisar Renhållningen till EDP futures funktioner, och detaljerna kring gallring beskrivs närmare i registerförteckningen. Renhållningen stödjer sig på den lagstiftning som finns och har även granskat hur andra organisationer gjort som använder EDP future.

Rekommendationer:

- *Färdigställ registerförteckningen avseende överföring av personuppgifter till mottagare utanför organisationen.*
- *Utvärdera var behandling, lagring och överföring av personuppgifter sker för de funktioner som bolaget använder och som är molnbaserade.*
- *Säkerställ att all behandling som finns i EDP-future återspeglas i registerförteckningen.*
- *Säkerställ att kännedom om var information lagras och behandlas när en underleverantör tillhandahåller en tjänst eller ett system, exempelvis i molnet.*

3.4 Dokumentation

Inom frågeområdet för dokumentation ligger Renhållningen på **3,3 av 4,0**.

I samband med den här granskningen har vi i huvudsak tagit del av följande dokumentation:

- IT Policy
- Integritetspolicy
- Digital kommunikation- instruktion för användarna
- Dokumenthanteringsplan
- Registerförteckning
- Personuppgifts- och gallringsplan EDP Future_210406
- Sociala Medier Policy_Draft IT
- Systemförteckning
- Cookie-definiering
- Dataskyddsombud_DraftIT
- Hantering personuppgifter_DraftIT
- Integritetspolicy Intern_DraftIT
- IT-Policy_DraftIT
- Mobiltelefonpolicy_DraftIT

- Riktlinjer fritextfält_DraftIT

I nuläget finns det en intern *integritetspolicy* och en *IT-policy* som ligger tillgängligt på bolagets intranät och stödverktyget kring dokumentation enligt GDPR, DraftIT. På hemsidan finns en externt riktad *personuppgiftspolicy* som i korthet redogör för bolaget behandling av personuppgifter. Rutiner som är mer specifika än integritetspolicyn kring hur Renhållningen hanterar personuppgifter finns enligt de intervjuade i personalhandboken.

Dokumentet *Hantering av personuppgifter* beskriver i hur Renhållningen skall respektera personuppgifter och vad som kan anses vara känsliga personuppgifter, vad en personuppgiftsbehandling innebär och hur dessa personuppgifter hanteras.

Bolaget har en mall för *personuppgiftsbiträdesavta*l (PUB-avtal), i den mån det kan bli aktuellt. Den mall som används för PUB-avtal och som idag är standard inom bolaget utgörs av en mall som framtagits av kommunen. Renhållningen har även ett PUB-avtal med VISMA som är utformat av VISMA.

Det är oklart om huruvida Renhållningen behandlar känsliga personuppgifter, annat än i förekommande fall avseende sina anställda. Bolaget har dock inga klara rutiner för att genomföra riskanalyser kopplat till behandlingen av känsliga personuppgifter. Rutiner och process för att kunna bemöta data subjektens förfrågan om deras rättigheter enligt GDPR finns idag inte dokumenterat. Renhållningen har idag inte en dokumenterad incidenthanteringsprocess eller rutiner kring hur en incident skall hanteras och kommer således att hantera personuppgiftsincidenter ad-hoc framgent.

När besökare besöker Renhållningen hemsida och läser integritetspolicyn blir de informerade om att Renhållningen använder samlar in cookies vid besök. Vidare beskriver inte stycket kring cookies vilken typ av cookie-teknik hemsidan använder samt vilka typer av personuppgifter som samlas in, behandlas, vilka leverantörer och under vilken tidsperiod.

Rekommendationer:
- *Förtydliga vilka personuppgifter Renhållningen behandlar gällande sina kunder/ besökare.*
- *Säkerställ att behandling av känsliga personuppgifter kartläggs och tillförs adekvat riskhantering.*
- *Ta fram en process för hantering av personuppgiftsincidenter.*
- *Förtydliga stycket om cookies i integritetspolicyn.*

3.5 Ansvar som personuppgiftsbiträde
Renhållningen hamnar här på **3,0 av 4,0**.

Renhållningen behöver behandla kundens uppgifter för att kunna tillhandahålla verksamhetens tjänst och tillgodose rätt service. Vidare tillhandahåller Renhållningen sina tjänster åt en annan kommun idag utöver Kristianstad kommun, och blir i detta fall personuppgiftsbiträde.

Bolaget har idag tillgång till Kristianstad kommuns personuppgiftsbiträdesavtal. Innan personuppgiftsbiträdesavtalet används kvalitetssäkrar Renhållningen innehållet med Kristianstad kommun, för att säkerställa att alla relevanta uppgifter finns med i den dokumentversion som används. I registerförteckningen framgår det endast när Renhållningen är personuppgiftsansvarig. Därav ser vi en avsaknad i dokumentation där Renhållningen agerar personuppgiftsbiträde och därmed en möjlig avsaknad i kartläggningen.

Rekommendationer:

- *Kartlägg när Renhållningen kan agera som personuppgiftsbiträde.*
- *Dokumentera kartläggningen.*

3.6 De registrerades rättigheter

För frågeområdet kring de registrerades rättigheter hamnar Renhållningen på **2,2 av 4,0**, vilket innebär att detta är det svagaste området för bolaget. Resultatet speglar avsaknaden av dokumenterade processer i form av styrdokument för att tillgodose de registrerades rättigheter.

Bolaget tillhandahåller generell information till sina kunder rörande insamlingen av personuppgifter på sin hemsida. Av informationen på hemsidan framgår bland annat vad kunden godkänner i hur personuppgifterna hanteras, vem som har tillgång till uppgifterna samt vilka rättigheter kunden har. Kunden kan även begära att Renhållningen rättar, raderar eller begära begränsning av användning. Av denna information framgår dock inte vilka personuppgiftsbehandlingar som utförs vid insamling av personuppgifter.

Om en registrerad person åberopar ett registerutdrag har Renhållningen ingen process på plats för att hantera detta. Process eller rutin för att rätta felaktiga eller radera personuppgifter finns inte heller dokumenterade, men bolaget uppger att om kunden kontaktar Renhållningen kring en felaktig personuppgift så skickas ärendet till IT-förvaltaren som korrigerar detta. Bolaget saknar även dokumenterade rutiner kring begränsning av specifika personuppgiftsbehandlingar, eller invändningar mot viss personuppgiftsbehandling. Rutiner för att den registrerade inte utsätts för automatiserat individuellt beslutsfattande anses inte behövas då Renhållningen inte använder sig av något automatiserat beslutsfattande.

Rekommendationer:

- *Redovisa vilka kategorier av personuppgifter som samlas in. Per område och hur det samlas in i respektive fall.*
- *Säkerställ att skriftlig rutin finns för utlämnande av registerutdrag.*
- *Säkerställ att skriftlig rutin finns för rättning och radering av personuppgifter.*
- *Säkerställ att dokumenterade rutiner finns kring när begränsning av specifika personuppgiftsbehandlingar, eller invändningar mot viss personuppgiftsbehandling kan bli aktuellt.*

3.7 Lagstiftning
Renhållningen hamnar här på **3,5 av 4,0**.

Avseende bevakning inom det legala området rörande personuppgiftsrelaterad lagstiftning använder bolaget kommunens jurister som stöd och bolaget får därmed genom denna resurs anses ha en utpekade funktion för omvärldsbevakning inom området. Utöver detta håller personer i ledande ställning inom bolaget sig uppdaterade genom löpande information som kommer till dem genom nyhetsbrev och olika forum.

3.8 Barn
Renhållningen hamnar här på **3,0 av 4,0**.

Renhållningen behandlar endast personuppgifter kring anställdas barn i den mån dessa uppgifter är införda i lönesystemet, exempelvis i samband med vård av barn, eller föräldraledighet. Renhållningen har beslutat om att anonymisera barnets namn och endast behålla personnumret, vilket finns lagrat i AGDA, VISMAs system.

3.9 Ostrukturerad data
Avseende området ostrukturerad data ligger resultatet för bolaget på **2,3 av 4,0**.

Utvärdering av ostrukturerad data har genomförts inför införandet av GDPR. Servrar och fildelningsytor är behörighetsstyrda och delas med kommunen, och Renhållningen och kommunen delar samma AD. Det finns både gemensamma eller personliga fildelningsytor men allt styrs av behörigheter.

De intervjuade vet på ett ungefär vilka personuppgifter som finns i ostrukturerad form men kan inte säkerställa att alla plattformar där detta sker är identifierade, vilket innebär att personuppgifter kan finnas lagrade utanför systemet. Det finns i nuläget inga dokumenterade rutiner eller riktlinjer kring ostrukturerad data, dess användning eller hur organisationen ska arbeta för att minska användningen av ostrukturerad data. Det finns därmed inte heller några gemensamma tekniska lösningar för att samordna organisationens ostrukturerade material.

Det arbete som sker inom området sker framförallt i muntlig form genom information till anställda. Bolaget framhåller att denna informationsspridning är ständigt pågående och att anställda regelbundet påminns om dataminimering och att med jämna mellanrum rensa personuppgifter från lokala arbetsytor, både fysiska och digitala.

Rekommendationer:

- *Fullfölj kartläggningen av förekomsten av ostrukturerad data och tillsätt nödvändiga dokumenterade policys och riktlinjer kring användningen av ostrukturerad data, samt åtgärder för att minska användningen av denna typ av data.*
- *Säkerställ vidare att medarbetarna utbildas kring hur minskning av användningen av ostrukturerad data kan uppnås.*

3.10 Säkerhetsåtgärder

Inom området säkerhetsåtgärder får Renhållningen **2,3 av 4,0**.

Renhållningen tar idag hjälp av kommunens upphandlingsenhet när det gäller att säkerställa att de systemstöd/ applikationer som köps in och implementeras har inbyggt dataskydd och dataskydd som standard. Det var dock ett tag sedan Renhållningen köpte in något nytt system.

Renhållningen genomför kontinuerligt kompetenshöjande insatser kring dataskydd genom att informera och påminna. Bolaget har även genomfört fysiska utbildningar för att öka kompetensen kring dataskydd.

Utifrån genomförda intervjuer framgår det att bolaget inte känner till om det finns någon dokumenterad rutin för att upptäcka och hantera personuppgiftsincidenter. Bolaget uppger att personuppgiftsincidenter hittills inte inträffat. I den dokumentation som tagits del av inom ramen för denna granskning har dock en kortare beskrivning av bolagets incidenthantering återfunnits i dokumentet *Digital kommunikation.* Den beskrivning av incidenthantering som återfinns i detta dokument får dock betraktas som knapphändig, då informationen som ges inte ger vägledning kring hur en personuppgiftsincident ska hanteras praktiskt. Vid en skarp personuppgiftsincident behövs det en tydligare bild av vad som behöver göras, och det är vidare delvis olika åtgärder som behöver vidtas vid en personuppgiftsincident än vid exempelvis en IT-incident, inte minst om rapporteringsskyldighet till tillsynsmyndighet föreligger. Renhållningen kan därmed inte anses ha en fullt ut definierad eller dokumenterad incidenthanteringsprocess.

Mitigerande aktiviteter för att hantera personuppgiftsincidenter hanterar Renhållningen idag ad-hoc då det inte finns konkret dokumentation på vad som skall göras eller hanteras. Vidare, använder Renhållningen Kristianstad kommuns dataskyddsombud som vid behov stödjer Renhållningen i dataskyddsrelaterade frågor, och därmed kan Renhållningen säkerställa att organisationen tillgodogör sig nödvändig information till men mån det behövs.

Rekommendationer:

- *Förtydliga incidenthanteringsrutin för personuppgiftsincidenter med konkreta åtgärder.*
- *Utbilda verksamheten i hur en personuppgiftsincident skall hanteras.*

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 med representanter från de delar av bolaget som anses vara representativa för kommunens arbete med GDPR. 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 "Ja". Organisationen ligger i flera fall över den grundnivå som som kan anses vara acceptabel vid införandet av GDPR, men får trots detta sägas ha förbättringspotential inom ett antal områden. Därför har, trots det grafiskt goda resultatet, ett 20-tal rekommendationer föreslagits i föregående avsnitt.

Renhållningen har en generell medvetenhet gällande GDPR och arbetar med att skydda personuppgifter på ett bra sätt. Bolaget har stöd från kommunens jurister i frågor kring dataskydd och andra regulatoriska frågor, liksom ifråga om användning av PUB-avtal. Bolaget använder sig av samma dataskyddsombud som Kristianstad kommun (JP Infonet).

Bolaget har vidtagit åtgärder och utbildat personal, men roller och ansvar kring dataskydd och informationssäkerhet är fortfarande inte fullt ut definierade i organisationen.

Renhållningen har en tydlig registerförteckning och en systemförteckning på plats som tydligt beskriver organisationens behandlingar kopplat till system. Däremot ser vi att systemförteckningen och registerförteckningen inte helt stämmer överens med varandra, vilket innebär att det förekommer behandlingar av personuppgifter som inte ännu förts in i registerförteckningen. En särskild utmaning berör de system som är molnbaserade där frågan om lagring och behandling sker inom EU/EES inte kan sägas vara fullt ut hanterad. Därför bör registerförteckningen kompletteras i detta avseende. Detsamma avser de situationer där bolaget agerar personuppgiftsbiträde, vilka inte heller är full ut dokumenterade.

Bolaget har inte fullt ut klassificerat sin information, vilket gör det svårt för bolaget att värdera både personuppgifter och annan känslig data utifrån ett systematiskt risk- och

säkerhetsarbete. Delvis till följd av detta har bolaget inte i nuläget fullt ut kunnat säkerställa att användningen av ostrukturerad data minimeras och har inte heller något sätt att följa upp detta.

Avseende personuppgiftsincidenter saknas rutiner som på ett tydligt sätt definierar vad som utgör en personuppgiftsincident och hur anställda ska gå tillväga i händelse av incident. Bolaget saknar vidare tydliga rutiner på högre nivå kring rapporteringsskyldiga personuppgiftsincidenter, exempelvis till Integritetsskyddsmyndigheten.

Avseende de registrerades rättigheter är en generell slutsats att tydligheten gentemot Renhållningens kunder behöver förbättras, och även dokumenteras i interna riktlinjer för att ge organisationen vägledning i arbetet. Detta gäller både avseende vilka uppgifter som samlas in och för vilket ändamål, men även frågor som berör den enskildes möjlighet till registerutdrag, rättning eller radering, eller andra begränsningar i behandlingen av personuppgifter.

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

Integritetsskyddsmyndighetens hemsida