Kristianstads kommun

KOMMUNREVISIONEN

2020-11-18

Kristianstads kommun
Kommunstyrelsen
Styrelsen för C4 Energi AB

Förstudie och nulägesbeskrivning avseende arbetet med införandet av GDPR

På uppdrag av de förtroendevalda revisorerna i Kristianstads kommun har PwC genomfört en förstudie avseende införandet av GDPR inom C4 Energi. 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.

Efter genomförd förstudie bedömer vi att det delvis sker ett ändamålsenligt och heltäckande arbete gällande GDPR bedrivits och har åtgärder vidtagits för att efterleva de nya reglerna.

Bedömningen grundas bland annat på att arbetet med en anpassning efter GDPR påbörjats, men ännu inte nått i mål inom alla delar av organisationen. En förklaring kan vara att den projektgrupp som initialt tillsattes numera inte finns kvar för att driva det löpande arbetet. Ett resultat av detta är att det fortfarande finns områden där bolaget ännu inte är i mål, exempelvis behandlingsregistret för Kundservice (och delvis för HR), samt avsaknad av policys, dokumentation och rutiner för vissa områden.

Utifrån genomförd förstudie lämnar vi nedan rekommendtioner till styrelsen för C4 Energi AB. Ytterligare rekommendationer finns i bifogad rapport.

- Överväg att införa en modell för informationsklassificering för att säkerställa att känslig data hanteras på ett säkert sätt.
- Överväg att systemägare också blir informationssäkerhetsansvariga för respektive system, under överinseende av IT-chef.
- Säkerställ att bolaget följer rekommendationerna i dataskyddsförordningens artikel 30 "Register över behandling" kring innehåll i behandlingsregister.
- Säkerställ att gallringsrutiner finns dokumenterade för specifika behandlingar och system inom C4 Energi.
- Utarbeta och anta en integritetspolicy för C4 Energi.
- Uppdatera dokumentet "Digital kommunikation - instruktion för användare" så att det överensstämmer med de krav som GDPR ställer och ger medarbetarna praktisk vägledning i den dagliga hanteringen av personuppgifter.
- Utvärdera ifall det behövs ett PUB-avtal mellan C4 Energi, C4 Elnät, Kristianstad Biogas och Kristianstads kommun.
- Överväg att granska personuppgifter om barn i de system som används, för att säkerställa att all information är anonymiserad och att eventuella fritextfält inte har använts för att dokumentera personuppgifter om barn.
- Överväg att dokumentera i form av riktlinjer hur bolagets hantering av ostrukturerad data (digital och fysisk form) sker och vilka regelbundna åtgärder som ska genomföras av medarbetare respektive bolaget för att säkerställa efterlevnad.

- Säkerställ att inbyggt dataskydd finns dokumenterat i bolagets upphandlings- och inköpspolicy, samt i riktlinjerna.
- Säkerställ att incidenthanteringsrutiner för personuppgiftsincidenter är på plats och övade inom hela organisationen.
- Uppdatera dokumentet "Informationssäkerhet" så att det innehåller rutiner för hantering av personuppgiftsincidenter, och uppdatera dokumentet i övrigt i enlighet med GDPR.

Rapporten överlämnas till styrelsen för C4 Energi AB för beaktande och till kommunstyrelsen för kännedom. Revisorerna önskar svar på genomförd granskning före den 26 februari år 2021.

För revisorerna i Kristianstads kommun

Sven Gunnar Linné
Ordförande

Göran Sevebrant
Vice ordförande

Arbetet med införandet av GDPR inom C4 Energi - en förstudie och nulägesbeskrivning

Linus Owman

Omid Asali

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 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 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 man göra en konsekvensbedömning och vidta lämpliga åtgärder för att reducera riskerna för eventuella skador.

I slutet av juni detta år (2020) publicerade tidningen “Aktuell Säkerhet” en debattartikel kring införandet av GDPR och aktuellt läge. Några korta citat hjälper till att belysa denna granskning 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 framtidsäkra 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

Kristianstads kommuns revisorer 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 energibolaget C4 Energi och därvid bilda sig en uppfattning om nuläget. Förstudien ingår i revisionsplanen för år 2020.

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, 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. Intervju har genomförts i gruppform tillsammans med bolagets HR-chef, IT-chef och Kundservice-chef.

2. Kartläggning

2.1 Bakgrund - införandet av GDPR

Arbetet med införandet av GDPR inom C4 Energi initierades av ledningsgruppen, där IT-avdelningen tog ansvar för IT-säkerhetsfrågor, HR-chef tog ansvar för personuppgifter avseende anställda och externa utbyten relaterade till HR, och Kundservice-chefen tog ansvar för personuppgifter avseende kunder och externa utbyten avseende exempelvis leverantörer. Projektgruppen bestod initialt av HR-chef och Kundservice-chef, då IT-chefbefattningen vid tillfället för införandet ännu inte var tillsatt. Under införandet av GDPR har externa jurister (exempelvis Jurab) regelbundet anlitats av C4 Energi.

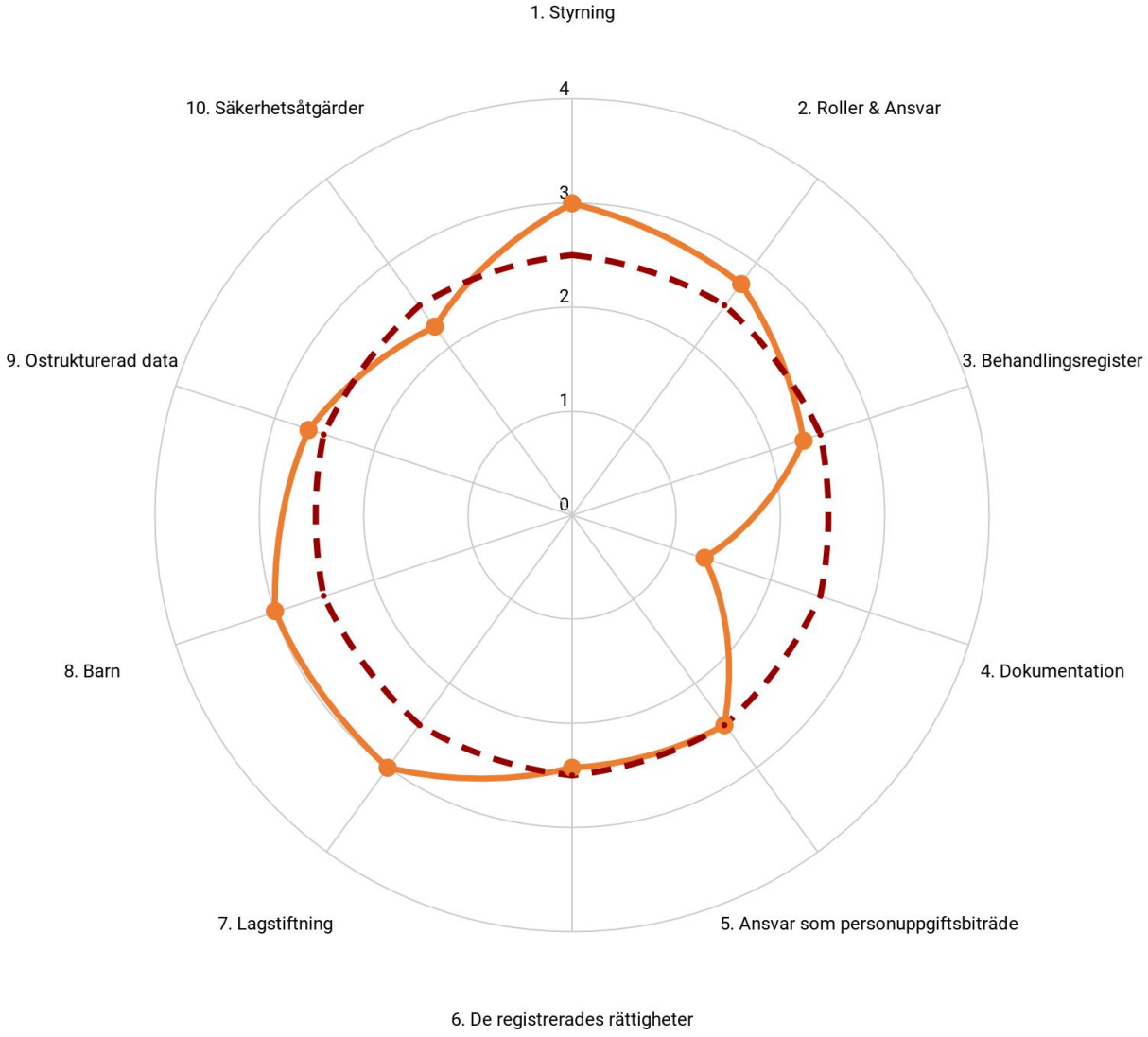
Projektgruppen finns inte kvar idag men C4 Energi arbetar löpande med dataskyddsfrågor inom respektive funktion, där funktionschef har ansvar för att uppfylla regelefterlevnad, med stöd av systemägare som har det yttersta ansvaret för att se till att ingen incident sker.

2.2 Övergripande resultat

För att sammanställa denna rapport har PwC intervjuat relevanta personer med insyn i C4 Energis 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 C4 Energis 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 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 C4 Energi har påbörjat ett arbete med att ta sig an de utmaningar som den nya dataskyddsförordningen innebär, men att detta arbete ännu inte gått helt i mål. Vi vill framförallt framhålla dokumentationsområdet och området för behandlingsregister som särskilt viktiga för det fortsatta arbetet. Bolaget ligger relativt nära den nivå som vi betraktar som grundnivå.

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 **3,0 av 4,0**. Det har funnits ett tydligt uppdrag att införa GDPR från ledningsgruppen. Arbetet har sedan drivits framåt av HR-chef, Kundservice-chef och IT-avdelningen, vilka varit dem som drivit det praktiska arbetet med införandet av GDPR framåt inom bolaget. HR-chef har fokuserat på personuppgiftsbehandlingar som avser personal och de datautbyten med externa parter som ligger inom ramen för detta område. Kundservice-chef har fokuserat på personuppgiftsbehandlingar som avser kunddata samt de datautbyten som sker med externa parter och leverantörer inom kundområdet. IT-avdelningen med IT-chef (ej tillsatt vid arbetets inledande), har ansvarat för personuppgiftsfrågor och informationssäkerhetsfrågor relaterat till systemkartan inom bolaget.

C4 Energi har löpande fått externt stöd från exempelvis juristfirman Jurab kring utbildningar och avtalsvillkor för personuppgiftsbiträdesavtal (PUB-avtal). Projektgruppen som en gång verkade finns inte kvar idag, utan arbetet med och ansvaret för regelefterlevnad av GDPR sker inom funktionerna. Jurab samt Draftits supportfunktioner inom Records- och Privacy-modulerna nyttjas löpande för att säkerställa omvärldsbevakning och ett fortsatt arbete för de delar som ej har fullständigt utvecklats.

Organisationen är uppmärksammad på dataskyddsarbetet vilket är en stående punkt på ledningsmöten tillsammans med informationssäkerhet.

Informationstillgångarna inom C4 Energi är inte klassificerade baserat på känslighet och öppenhet och en kartläggning har inte utförts. Bolagets IT-policy (2017) säger att “informationstillgångar som klassificerats utifrån risk ska skyddas med ändamålsenliga kontroller för IT-säkerhet för att säkerställa behörig åtkomst till information inom C4 Energi”, men en regelrätt informationsklassificering har ännu inte skett, enligt IT-chef. IT-avdelningen utövar monitorering av IT-landskapet och kontroll på hur data behandlas, med larm om olovliga eller misstänkta aktiviteter. Det finns också skanningsverktyg och behörigheter i IT-miljön för att säkerställa att personuppgifter inte utnyttjas eller når obehöriga inom och utanför C4 Energi.

Rekommendation:

- Överväg att införa en modell för informationsklassificering för att säkerställa att känslig data hanteras på ett säkert sätt.

3.2 Roller och ansvar

Inom området roller och ansvar har bolaget erhållit resultatet **2,8 av 4,0**. Bolaget har utvärderat om en roll som dataskyddsombud är nödvändigt och landat i ett informellt beslut om att detta inte är nödvändigt för C4 Energi. Beslutsprocessen kring detta har inte dokumenterats. Det är idag IT-chefen som ansvarar för informationssäkerhet, men det finns

ingen dedikerad resurs som följer upp dataskyddsarbetet för bolaget och ser till att regelefterlevnad kring GDPR säkerställs löpande, utan detta sker av funktionerna (HR, Kundservice, och IT).

Systemansvariga är IT-chef, HR-chef och Kundservice-chef vilka också ansvarar för övriga frågor gällande GDPR inom sina respektive områden, men där HR och Kundservice inte har något ytterligare ansvar för informationssäkerhet.

Rekommendation:

- Överväg att skapa löpande avstämningar i helgrupp för de funktioner som har ett ansvar för GDPR. På detta sätt kan goda exempel och praktiker från olika delar av verksamheten snabbt få genomslag på andra håll. Dessutom skapas ett helhetsgrepp på frågorna inom organisationen, där de olika funktionerna inte är utlämnade åt sig själva, utan hjälps åt med både implementering och uppföljning av regelefterlevnad. Dessutom skapas en bredare förståelse kring hur arbetet med GDPR även påverkar frågor kring informationssäkerhet i ett bredare perspektiv.

- Överväg att systemägare också blir informationssäkerhetsansvariga för respektive system, under överinseende av IT-chef.

- Dokumentera och motivera valet att inte tillsätta funktionen som dataskyddsombud och säkerställ vidare att de ansvarsområden som regleringen tillskriver ett dataskyddsombud (dataskyddsförordningen art. 37-39) tillgodoses genom de funktioner som i nuläget har ett utpekat ansvar. Utbilda om nödvändigt ytterligare personer med utpekat ansvar för att säkerställa uppdaterad kunskap inom organisationen.

3.3 Behandlingsregister (registerförteckning)
För detta område har bolaget erhållit ett resultat på **2,3 av 4,0**. Olika delar av organisationen har nått olika långt i färdigställandet av ett behandlingsregister. På HR-sidan har arbetet kommit längre, men vissa delar saknas fortfarande (se rekommendationerna nedan). På Kundservice och Ekonomi är upprättandet av ett behandlingsregister påbörjat, men befinner sig fortfarande i ett skede där relativt många uppgifter fortfarande saknas. Eftersom den stora delen av personuppgiftsbehandlingar sker inom Kundservice (med c:a 28000 abonnenter), och då behandling av extern data generellt sett utgör en högre risk för bolaget, innebär detta att poängbedömningen inom detta område främst baserats på det arbete som genomförts inom Kundservice (även om HR-sidan kommit längre).

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

Det finns gemensamma system för hela koncernen, exempelvis Lime CRM och BFUS, vars behandlingar täckts in i de behandlingsregister som upprättats inom HR och Kundservice. För de behandlingar som sker i dotterbolagen, i system som inte är koncerngemensamma, är bilden som getts vid intervjuer inte helt tydlig kring huruvida det finns behandlingsregister på plats.

Det behöver utredas huruvida C4 Elnät AB, Kristianstads Biogas AB och C4 Energi AB har ett delat personuppgiftsansvar. Behandlingsregister ska dock upprättas även för dessa delar, i den mån detta inte redan är på plats.

Rekommendation:

- Säkerställ att bolaget följer rekommendationerna i dataskyddsförordningens artikel 30 “Register över behandling” kring innehåll i behandlingsregister. I nuläget saknas vissa delar, exempelvis tekniska och organisatoriska åtgärder, definierade tröskelvärden för när radering ska ske, huruvida organisationen är personuppgiftsansvarig eller personuppgiftsbiträde (oavsett om behandlingen sker gentemot är intern eller extern part) etc.

- Säkerställ att arbetet med behandlingsregistret färdigställs för de delar av organisationen där detta ännu inte skett, exempelvis Kundservice.

- Säkerställ att arbetet med behandlingsregister färdigställs för de delar av koncernen, och för de delar som avser system som inte är koncerngemensamma.

- Säkerställ att gallringsrutiner finns dokumenterade för specifika behandlingar och system inom C4 Energi.

- Bolaget har infört Daftit som ett sätt att ta del av supportfunktioner, mallar och skrivningar kring dataskydd. Dock används inte Draftits funktion kring att bygga ett automatiserat behandlingsregister. Givet hur arbetet med skapandet av behandlingsregister fortskrider hade möjligen en förbättring kunnat vara att även använda dessa delar i Draftit, eller annat liknande program, då detta underlättar både arbete med och monitorering av efterlevnad.

3.4 Dokumentation

Inom frågeområdet för dokumentation ligger bolaget på **1,3 av 4,0**, vilket innebär att detta är det svagaste området för bolaget.

I nuläget saknas en integritetspolicy för C4 Energi. Integritetspolicy som dokument riktar sig inte enbart mot bolagets kunder, utan förklarar på ett transparent sätt den mission organisationen aktivt arbetar efter för att säkerställa att den personliga integriteten inte kränks. Integritetspolicyn utgör således en bolagsövergripande viljeyttring, vilket även skapar medvetenhet för de anställda.

Bolaget saknar i nuläget även ytterligare riktlinjer för sina anställda kring behandlingen av personuppgifter. Dokumentet “GDPR C4 Energi” är endast en sammanfattning av området GDPR och dess bestämmelser, men innehåller ingen ytterligare information kring den dagliga hanteringen av personuppgifter ute i organisationen. Dokumentet “Digital kommunikation - instruktion för användare” är från 2015 och innehåller översiktliga instruktioner som berör den gamla Personuppgiftslagen.

Det finns en mall för personuppgiftsbiträdesavtal att tillgå via Jurab eller Draftit, men oftast används leverantörernas mallar.

Rekommendation:

- Utarbeta och anta en integritetspolicy för C4 Energi.
- Uppdatera dokumentet “Digital kommunikation - instruktion för användare” så att det överensstämmer med de krav som GDPR ställer och ger medarbetarna praktisk vägledning i den dagliga hanteringen av personuppgifter. Säkerställ att innehållet i det uppdaterade dokumentet speglar innehållet i integritetspolicyn.

3.5 Ansvar som personuppgiftsbiträde

Bolaget hamnar här på **2,5 av 4,0**. Bolaget agerar sällan personuppgiftsbiträde till andra organisationer, men har identifierat de tillfällen då detta sker. Det finns även mall för personuppgiftsbiträdesavtal.

Som tidigare nämnts framgår inte i behandlingsregistret för vilka behandlingar C4 Energi agerar som personuppgiftsbiträde eller som personuppgiftsansvariga (se 3.3). Enligt vad vi erfar är det inte helt klarlagt om C4 Energi, C4 Elnät och Kristianstad Biogas AB har ett delat personuppgiftsansvar eller inte, vilket innebär att frågan om huruvida det behövs ett PUB-avtal som reglerar datautbytet mellan bolagen inom koncernen behöver utredas (detta oaktat ett gemensamt AD, då bolagen har olika organisationsnummer).

De PUB-avtal som presenterats för C4 Elnät, C4 Energi och Biogas avser endast ett avtal med Skandikon kring tjänstepensioner, dvs de utgör personuppgiftsbiträdesavtal för externa leverantörer, men reglerar inte utbytet inom koncernen.

Rekommendation

- Utvärdera ifall det behövs ett PUB-avtal mellan C4 Energi, C4 Elnät, Kristianstad Biogas och Kristianstads kommun.

3.6 De registrerades rättigheter

För frågeområdet kring de registrerades rättigheter hamnar bolaget på **2,4 av 4,0**.

Bolaget har information på hemsidan kring hur behandlingen av personuppgifter sker och var den registrerade kan vända sig med frågor.

Om en registrerad person åberopar en rättighet, exempelvis radering, har C4 Energi systemstöd för att tillhandahålla det som efterfrågas. Om en kund behöver rätta sina uppgifter kan detta göras av kunden direkt via C4 Energis kundportal.

Avseende personaldata, raderas alla personer som avslutar sin anställning på C4 Energi, utom i de delar som krävs för att fullgöra bolagets skyldigheter inom annan tillämplig lagstiftning, exempelvis arkivlagen.

Det som saknas i kommunikationen till de registrerade på hemsidan är tydlighet kring den behandlingen bolaget utför. På hemsidan finns det även cookies som går att acceptera men vilka cookies och hur dessa beter sig finns inte tillgängligt för besökare av webbplatsen.

Det finns ingen dokumenterad process för hur registerutdrag lämnas ut, hur rättning eller radering av felaktiga personuppgifter sker även om organisationen är medveten om hur det ska utföras.

Rekommendation:

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

- Säkerställ att definiera hemsidans cookies.

3.7 Lagstiftning

Bolaget hamnar här på **3,0 av 4,0**. C4 Energi har extern hjälp med omvärldsbevakning från bland annat Jurab juristfirma samt Draftit och även Energimyndigheten, och övervakning sker delvis aktivt inom detta område. Om förändringar blir relevanta för C4 Energi initieras ett arbete för att uppnå kravet.

Rekommendation:

- Tillse att påverkan från lagstiftning inom området får fullt genomslag i organisationen.

3.8 Barn

Bolaget hamnar här på **3,0 av 4,0**. Bolaget behandlar idag ett fåtal uppgifter gällande barn. Behandlingen där uppgifter om barn ingår avser bolagets åtagande gentemot sina anställda avseende lagstadgade krav kring föräldrapenning. För dessa behandlingar är hålls endast anonymiserade uppgifter om barnets födelseår.

Rekommendation:

- Överväg att granska personuppgifter om barn i de system som används, för att säkerställa att all information är anonymiserad och att eventuella fritextfält inte har använts för att dokumentera personuppgifter om barn.

3.9 Ostrukturerad data

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

Bolagets IT-landskap använder sig primärt av Office 365 där ostrukturerad data skannas av och övervakas. IT-chefen larmas om det sker transaktion av ostrukturerad data som anses vara utanför bolagets verksamhetsbeteende. Dock saknas rutiner för att minska behandlingen av ostrukturerad data.

När en anställd slutar tas alla filer och data bort för den anställde. Denna process utförs av IT-avdelningen men är inte dokumenterad.

Personalen har utbildats kring hur de ska minimera användningen av ostrukturerad data. Bolaget har informerat anställda kring vad som gäller för hantering av ostrukturerad data, men det finns inga dokumenterade riktlinjer kring detta.

Utöver detta finns ostrukturerad data i pärmar och akter, men systematiken kring hur denna ostrukturerade data kan minimeras är ännu inte färdigställd.

Rekommendation:

- Överväg att dokumentera i form av riktlinjer hur bolagets hantering av ostrukturerad data (digital och fysisk form) sker och vilka regelbundna åtgärder som ska genomföras av medarbetare respektive bolaget för att säkerställa efterlevnad.

- Överväg att ta fram en rutin för att säkerställa personalens hantering av ostrukturerad data.

3.10 Säkerhetsåtgärder

Inom området säkerhetsåtgärder får bolaget **2,3 av 4,0**. Bolaget har för vissa leverantörer en instruktion i PUB-avtalet (eller i bilaga) där säkerhetsåtgärder definieras och beaktas avseende ett specifikt system. I bolagets IT-strategi (2017) anges att “leverantörer ska agera proaktivt för att säkerställa att kontroller för IT-säkerhet är operativa i linje med verksamhetens krav”.

Avseende upphandling och systemutveckling finns idag dock ingen formaliserad rutin inom bolaget för att säkerställa inbyggt dataskydd eller dataskydd som standard, varken i upphandlingspolicy (2018), i riktlinjer för upphandling och inköp (2018) eller i inköpspolicy (2015). Frågan om inbyggt dataskydd eller dataskydd som standard beaktas istället löpande av den person som driver den enskilda upphandlingen.

Avseende utbildning av de anställda är Junglemap det system som används för att hantera utbildning och medvetenhetshöjande frågor kring säkerhet. Det skickas regelbundet ut utbildningsmoduler till anställdas mail där detaljerad information redovisas efter respondenten har svarat. C4 Energi har också överblick kring hur respondenterna har besvarat frågorna och kan därefter förstå hur medveten i organisationen ser ut. Att besvara frågorna från Junglemap är ett krav inom organisationen och på ledningsgruppsmöten.

Avseende hanteringen av eventuella personuppgiftsincidenter finns idag ingen dokumenterad rutin för detta. Hanteringen av personuppgiftsincidenter inryms istället inom de gängse incidenthanteringsrutiner som avser bolagets IT-miljö, men dessa innehåller inte specifika rutiner som täcker in personuppgiftsincidenter (se exempelvis dokument “Informationssäkerhet” ej daterat, samt dokument “Digital kommunikation - instruktion för användare, 2015). Dokumentet “Informationssäkerhet”, vilket är det dokument som tydligast hanterar incidenthanteringen inom bolaget, innehåller inga specifika anvisningar för hanteringen av en personuppgiftsincident. Vidare avspeglar dokumentet inte incidenthanteringsprocessen efter GDPRs införande, då Datainspektionen inte nämns som den tillsynsmyndighet till vilken incidentrapportering ska ske. Detta innebär att det i praktiken saknas rutiner och praktisk vägledning för hur bolaget ska agera vid en

personuppgiftsincident. Den incidenthanteringsprocess som finns inom bolaget är, enligt de intervjuade, inte övad.

Rekommendation:

- Säkerställ att inbyggt dataskydd finns dokumenterat i bolagets upphandlings- och inköpspolicy, samt i riktlinjerna.
- Säkerställ att incidenthanteringsrutiner för personuppgiftsincidenter är på plats och övade inom hela organisationen.
- Uppdatera dokumentet “Informationssäkerhet” så att det innehåller rutiner för hantering av personuppgiftsincidenter, och uppdatera dokumentet i övrigt i enlighet med GDPR.

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 bolagets 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 "delvis". Liksom inom andra områden finns det alltid utrymme för förbättringar och rekommendationer har föreslagits i föregående avsnitt.

Bolaget har generellt sett tagit sig an frågorna kring skyddet av personuppgifter och beaktat flera delar av GDPR, även om ett fullständigt behandlingsregister inte finns på plats för alla delar av bolaget. Åtgärder har vidtagits genom utbildningsverktyg för att säkerställa att medvetenhets- och kunskapshöjande insatser kring personuppgiftsbehandling.

Bolaget har en struktur med roller och ansvar som för att fortsätta med dataskyddsarbetet. Ledningsgruppen har ett intresse i utvecklingen av dataskyddsarbetet och dataskydd är på agendan på varje ledningsgruppsmöte, under den punkt som berör IT.

Bedömningen baserat på den översiktliga förstudie som genomförts är att arbetet med en anpassning efter GDPR påbörjats, men ännu inte nått i mål inom alla delar av organisationen. En förklaring kan vara att den projektgrupp som initialt tillsattes numera inte finns kvar för att driva det löpande arbetet. Ett resultat av detta är att det fortfarande finns områden där bolaget ännu inte är i mål, exempelvis behandlingsregistret för Kundservice (och delvis för HR), samt avsaknad av policys, dokumentation och rutiner för vissa områden.

Beslutet att inte tillsätta ett dataskyddsombud kan ha inneburit att det löpande arbetet med att övervaka efterlevnaden inom området kommit att nedprioriteras i den dagliga

verksamheten efter att införandedatum passerat, då de funktioner som har detta ansvar behöver fokusera på löpande drift och frågor kopplade till denna.

Ett sätt att ta ett strukturerat helhetsgrepp kring frågan skulle kunna vara att skapa löpande avstämningar i gruppform där den projektgrupp som initialt hade ansvar för införandet åter aktiveras för att driva det löpande arbetet med dataskydd framåt (se även 3.2).

Bolaget skulle vidare vara betjänt av att koppla arbetet med skyddet av personuppgifter till ett bredare informationssäkerhetsarbete, vilket kan ske genom att systemägarna i samråd med IT-chef involveras i arbetet. På så vis kopplas arbetet med GDPR till informationssäkerhet samt till bolagets övriga arbete med risk- och sårbarhetsanalyser.

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

Datainspektionens hemsida