Granskningsrapport
Genomförd på uppdrag av revisorerna
18/2021-2

Sundbybergs stad

Uppföljande granskning av stadens informationssäkerhet samt följsamhet gentemot GDPR

Building a better working world

Innehållsförteckning

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna följt upp två av de fördjupade granskningar[1] och en uppföljning[2] som genomfördes i Sundbybergs stad under revisionsåren 2019 och 2020. Kommunstyrelsen bedöms sammanfattningsvis delvis ha beaktat revisorernas iakttagelser och rekommendationer, samt vidtagit relevanta åtgärder av lämnade rekommendationer. I flera fall konstaterar vi att ett arbete pågår och en del rekommendationer därför inte har beaktats fullt ut. I flera fall har revisorernas rekommendationer varken beaktats eller åtgärdats, däribland kvarstår vissa brister som vi bedömer vara av allvarlig karaktär.

Bland kvarstående brister vill vi bland annat lyfta fram att vi anser det vara allvarligt att ett beslutat och kommunicerat ledningssystem för informationssäkerhet fortsatt saknas. Det är inte ett lagstadgat krav att implementera ett ledningssystem för informationssäkerhet, men det kan enligt vår bedömning dels betraktas som vedertagen praxis, dels ha en betydande inverkan på resterande delar i stadens informationssäkerhetsarbete. Resultatet är att Sundbybergs stad fortsatt saknar flertalet grundläggande komponenter för att säkerställa ändamålsenlig informationssäkerhetsstyrning, däribland en informationssäkerhetsspecifik organisationsstruktur, adekvata uppföljningar samt en formulerad stadsövergripande process för åtkomsthantering.

Vår sammanfattande bedömning är således att kommunstyrelsen inte har nått tillräckligt långt i arbetet vad gäller informationssäkerhet mot bakgrund av tidigare lämnade rekommendationer. Detta även fast relativt lång tid har förflutit sedan tidigare granskningar. Det kvarstår därför ett omfattande arbete för att åtgärda de rekommendationer som endast delvis, alternativt inte alls, har beaktats.

I tabellen nedan redovisas en sammanställning av uppföljningen med angivelse av huruvida tillräckliga åtgärder vidtagits till följd av lämnade rekommendationer.

Granskning	Antal rekommendationer	Åtgärdad		
		Ja	Delvis	Nej
Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering (KS-0486/2019)	13	3	5	5
Granskning av efterlevnad - Dataskyddsförordningen GDPR (KS-0258/2020)	5	2	2	1
TOTALT	**18**	**5**	**7**	**6**

Granskningen omfattar även uppföljning av stadens åtgärder med anledning av Schrems II

[1] De två fördjupade granskningarna avser "Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering" samt "Granskning av efterlevnad – Data skyddsförordningen GDPR".
[2] Uppföljning av stadens åtgärder med anledning av Schrems II (C311/18) "Överföring av personuppgifter till tredjeland".

(C311/18) "Överföring av personuppgifter till tredjeland". Vår bedömning är att kommunstyrelsens utredning förefaller vara gediget utförd, med analys av rätts- och omvärldsläget, samt ett övervägande av alternativa tjänster. Riskerna med att direkt avsluta ett stort antal tjänster vägs mot riskerna med att under en övergångsperiod fortsätta använda tjänsterna för att under ordnade former finna andra lösningar. Utredningens ställningstagande att inte omedelbart avsluta nuvarande tjänster, men att omgående vidta åtgärder för att hantera befintliga risker, framstår som ändamålsenligt givet stadens utgångsläge, samt de generellt oklarheter som ännu finns kring effekterna av Schrems II. Ytterligare definiering av tidplan för åtgärder är inte känt vid tidpunkten för granskningen.

Sundbyberg den 16 februari 2022.

Madeleine Gustafsson
EY

David Leinsköld
EY

1. Inledning

1.1. Bakgrund

Under 2019 genomförde revisionen en granskning av stadens informationssäkerhet. I granskningen noterades tydliga brister i stadens styrning och arbetssätt. Ett år senare genomfördes en granskning av stadens efterlevnad av GDPR. Även denna granskning visade på brister i stadens styrning, kontroll och uppföljning.

Med anledning av noterade brister i tidigare granskningar har revisionen beslutat att genomföra en uppföljande granskning med syftet att följa upp om staden vidtagit åtgärder utifrån revisionens lämnade rekommendationer.

1.2. Syfte och omfattning

Syftet med uppföljningen är att bedöma om de åtgärder som vidtagits inom identifierade förbättringsområden samt resultaten som uppnåtts är tillräckliga utifrån revisorernas givna rekommendationer. Granskningen omfattar uppföljning av följande fördjupade granskningar:

- Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering
- Granskning av efterlevnad - Dataskyddsförordningen GDPR

Granskningen omfattar även uppföljning av stadens åtgärder med anledning av Schrems II (C311/18) "Överföring av personuppgifter till tredjeland".

1.3. Metod och genomförande

Dokument som rör kommunstyrelsens åtgärder har analyserats utöver avstämningar med ansvariga tjänstemän.

2. Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering

Granskningen syfte var att ge en övergripande nulägesbild om huruvida kommunstyrelsen har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

I granskningen konstateras att den centrala uppföljningen av arbetet med informationssäkerhet utgör ett tydligt förbättringsområde. Brister identifierades i hur nämnder hanterar bl.a. upphandlingar, avtal med externa leverantörer, utför informationsklassningar, upprättar driftsinformation för verksamhetsspecifika IT-system, kontinuitetsplaner och hanterar personuppgifter. Vidare noteras att formella rapporteringsvägar inte definierats mellan stadens koncernbolag och stadsledningskontoret samt den centrala informationssäkerhetsfunktionen. I praktiken innebär det att stadsledningskontoret saknar insyn i hur koncernbolagen arbetar med informationssäkerhet, både som helhet och för viktiga enskilda initiativ såsom informationsklassning, systemförvaltning och arbetet med dataskyddsförordningen GDPR.

Vid tiden för granskningen var informationssäkerhetsarbetet begränsat till ett fåtal stadscentrala resurser. En sådan organisationsstruktur bedömdes inte vara ändamålsenlig för att bedriva ett tillfredsställande informationssäkerhetsarbete. Det bedömdes även saknas tillräckliga utbildningsinsatser inom informationssäkerhetsområdet.

Incidenthanteringsprocessen utgörs av detaljerade anvisningar för hur stadens "Service Desk" (hjälpcenter) ska hantera principer. Det bedömdes dock saknas en tydlig beskrivning av tillämpbart processflöde med korrelerande roller, ansvar och rapporteringskrav för kritiska incidenter som riskerar att orsaka mer allvarliga förluster av informationstillgångar.

I syfte att stärka stadens interna kontroll rörande informationssäkerhet presenterades i rapporten ett antal rekommendationer:

1. Tillse att adekvata kontroller och rutiner för uppföljning och efterlevnad mellan stadsledningskontoret och verksamheterna definieras, samt att designerade informationssäkerhetsroller tas fram och tillsätts i verksamheterna för ökad samverkan med den centrala informationssäkerhetsfunktionen.
2. Tillse att koncernbolagens arbete med informationssäkerhet aktivt följs upp och ökar kraven på återrapportering till stadsledningskontoret, alternativt även inkorporerar bolagen i den övergripande styrmodellen för informationssäkerhet.
3. Tillse att en informationssäkerhetsspecifik organisationsstruktur definieras och beslutas.
4. Tillse att roller och ansvar mellan stadsledningskontorets informationssäkerhetsfunktion och IT-enhet tydliggörs, samt att regelbundna forum för samverkan kring informationssäkerhetsrelaterade utmaningar och uppföljning av planerade initiativ inrättas.
5. Tillse att nivån av medvetande och involvering i stadens informationssäkerhetsarbete sprids inom både stadsledningskontoret och i verksamheterna, exempelvis genom formaliserade utbildningsinitiativ, samt att fler designerade informationssäkerhetsroller tas fram och tillsätts centralt och i

verksamheterna.

6. Tillse att en utbildningsplan för informationssäkerhet formaliseras. Denna bör innefatta genomförande av obligatoriska och regelbundna utbildningar inom informationssäkerhet med uppföljning av deltagande. Kommunstyrelsen rekommenderas även tillse att kommunikation och signering av användaranvisningen för nyttjande av stadens IT-miljö säkerställs.
7. Tillse att en stadsövergripande process för åtkomsthantering formaliseras, inklusive tydliga tilldelnings- och borttagningsförfaranden av behörigheter.
8. Tillse att stadsövergripande kontroller utformas för standardisering av genomförande av periodiska genomgångar. Kommunstyrelsen rekommenderas också tillse att förteckningar eller matriser skapas kring vilka behörigheter som inte är lämpliga att kombinera inom och mellan kritiska IT-system.
9. Tillse att ett tydligt processflöde för hantering av kritiska incidenter, inklusive roller, ansvar och rapporteringskrav, definieras som del av stadens incidenthanteringsprocess.
10. Tillse att en stadsövergripande process för hantering av programförändringar formaliseras, inklusive kontroller för säkerställande av ändamålsenlig ansvarsfördelning i införandet av programförändringar.
11. Tillse att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till stadens användare med en bestämd frekvens.
12. Tillse att kontinuitetsplaner utformas för samtliga verksamhetssystem som i genomförd informationsklassning har bedömts som skyddsvärda, samt att samtliga kontinuitetsplaner samlas ihop på Stadsledningskontorsnivå för central kvalitetssäkring och koordinering av regelbunden testning av kontinuitetsplanerna.
13. Tillser att en fullständig registerförteckning upprättas.

2.1. Uppföljning av vidtagna åtgärder

Nedan följer i tur och ordning rekommendation, tidigare lämnat svar på rekommendation i samband med granskningen, uppföljning av vidtagna åtgärder samt vår bedömning – dvs. hur väl rekommendationen har beaktats.

Rekommendation 1: Tillse att adekvata kontroller och rutiner för uppföljning och efterlevnad mellan stadsledningskontoret och verksamheterna definieras, samt att designerade informationssäkerhetsroller tas fram och tillsätts i verksamheterna för ökad samverkan med den centrala informationssäkerhetsfunktionen.

Svar på rekommendation 1: Kommunstyrelsen svarar att stadsledningskontoret under 2020 kommer att ta fram rutiner för uppföljning av informationssäkerheten inom hela förvaltningsorganisationen. En viktig komponent i detta uppföljningsarbete kommer bli att sprida kunskapen om hur SKL:s klassificeringsverktyg KLASSA används i identifieringen och riskhanteringen av de informationsmängder som staden behandlar. KLASSA ska också ligga till grund för framtida kontinuitetsplanering.

Uppföljning av vidtagna åtgärder per december 2021: EY:s uppföljning av vidtagna åtgärder kan inte se att kommunstyrelsens svar från 2020 vad gäller framtagandet av rutiner för uppföljning av informationssäkerheten inom nämnder och styrelser i helägda bolag har implementerats. Vi kan konstatera att kommunstyrelsen inte har tillsett att det finns formaliserade kontroller och rutiner för att följa upp arbetet med informationssäkerhet i stadens nämnder och styrelser i helägda bolag. Kommunstyrelsen

behöver säkerställa att adekvata kontroller och rutiner för uppföljning och efterlevnad mellan kommunstyrelsen och nämnderna samt styrelserna i helägda bolag definieras framgent. Ett dataskyddsombud (DSO) i personunion för samtliga nämnder har tillsatts från och med juni 2021 genom en konsultlösning. DSO har en instruktion som bland annat beskriver roller, uppgifter och arbetssätt för att säkerställa att stadens personuppgiftsansvariga nämnder har en god hantering av personuppgifter. En informationssäkerhetssamordnare anställdes i juni 2021 på kommunstyrelsens förvaltning, men avslutade sin tjänst i november 2021. Tjänsten är således vakant. En rekryteringsprocess har enligt stadsledningskontoret startats.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Bedömningen grundar sig på att kommunstyrelsen inte har tillsett att det finns formaliserade kontroller och rutiner för att följa upp arbetet med informationssäkerhet i stadens nämnder och styrelserna i helägda bolag. Vad gäller designerade och kommunicerade informationssäkerhetsroller på nämnder och styrelser i helägda bolag så saknas beslut om organisatoriskt förslag. Ett dataskyddsombud har tillsats. Vidare har en informationssäkerhetssamordnare tillsats men avslutat sin tjänst. Vi bedömer det väsentligt att kommunstyrelsen säkerställer ett tjänstemannastöd i den omfattning som krävs för att styrelsen ska kunna fullfölja sina åliggande med att leda, styra och följa upp arbetet.

Rekommendation 2: Tillse att koncernbolagens arbete med informationssäkerhet aktivt följs upp och ökar kraven på återrapportering till stadsledningskontoret, alternativt även inkorporerar bolagen i den övergripande styrmodellen för informationssäkerhet.

Svar på rekommendation 2: Kommunstyrelsen instämmer i revisorernas bedömning och planerar att se över området under 2020. För att kunna upprätta uppföljning av informationssäkerhetsarbetet inom hela kommunkoncernen behöver ett ledningssystem för informationssäkerhet fastställas. Med ledningssystemet på plats bedömer kommunstyrelsen att uppföljningsarbetet uppfyller den rekommendation som revisorerna lämnat.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen kan vid uppföljningen inte redovisa ett beslutat och kommunicerat ledningssystem för informationssäkerhet. Därför brister kommunstyrelsens uppföljning av informationssäkerhetsarbetet. Ledningssystemet ska utgå från informationssäkerhetspolicyn som i sin tur konkretiseras i riktlinjer och rutiner.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats. Beslutat och kommunicerat ledningssystem för informationssäkerhet saknas. Koncernbolagens arbete med informationssäkerhet följs därför inte aktivt upp av kommunstyrelsen.

Rekommendation 3: Tillse att en informationssäkerhetsspecifik organisationsstruktur definieras och beslutas.

Svar på rekommendation 3: Kommunstyrelsen instämmer i revisorernas bedömning och planerar att se över detta under 2019. Kommunstyrelsen hänvisar till ett förslag på

organisering av arbetet med informationssäkerhet som stadsledningskontoret har tagit fram. Arbetet ligger i linje med rekommendation 5.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen hänvisar till *Policy för informationssäkerhet* samt till *Program för krisberedskap och civilt försvar 2019–2022, kap. 4.3.5 Informationssäkerhet*, där en stadsövergripande ansvarsfördelning finns fastslagen. Kommunstyrelsen uppger dock att en beslutad och implementerad informationssäkerhetsspecifik organisationsstruktur saknas, men bör definieras och beslutas.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. *Policy för informationssäkerhet* beskriver bland annat roller och ansvar för att upprätta informationssäkerheten i Sundbyberg stad. I kapitel 4.3.5 *Informationssäkerhet* i *Program för krisberedskap och civilt försvar 2019–2022* utvecklas varför ett gott informationssäkerhetsarbete är viktigt. Däremot har kommunstyrelsen inte beslutat och implementerat en informationssäkerhetsspecifik organisationsstruktur i nämnder och styrelser i helägda bolag.

Rekommendation 4: Tillse att roller och ansvar mellan stadsledningskontorets informationssäkerhetsfunktion och IT-enhet tydliggörs, samt att regelbundna forum för samverkan kring informationssäkerhetsrelaterade utmaningar och uppföljning av planerade initiativ inrättas.

Svar på rekommendation 4: Kommunstyrelsen beskriver att stadsledningskontoret har tagit fram ett organisatoriskt förslag som möter rekommendationen om fler designerade informationssäkerhetsroller.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen hänvisar till dokumentet ”Praktisk hantering av beslutsfrågor rörande IT-säkerhet”. Där finns roller och ansvar tydliggjorda. Av dokumentet framgår att staden har tillsatt SÄK IT (Säkerhet och IT) i syfte att gemensamt ta fram väl avvägda IT-säkerhetslösningar. Det är en samarbetsgrupp för att bereda och utveckla IT- och informationssäkerhetsfrågor men hela stadens perspektiv. IT-strategigruppen består av säkerhetsskyddschef, dataskyddsombud (DSO), IT-driftchef och IT-infrastruturansvarig.

Vår bedömning: Vi bedömer att rekommendationen *har* beaktats. I dokumentet ”Praktisk hantering av beslutsfrågor rörande IT-säkerhet” tydliggörs roller och ansvar samt en beskrivning av ett forum för samverkan beskrivs.

Rekommendation 5: Tillse att nivån av medvetande och involvering i stadens informationssäkerhetsarbete sprids inom både stadsledningskontoret och i verksamheterna, exempelvis genom formaliserade utbildningsinitiativ, samt att fler designerade informationssäkerhetsroller tas fram och tillsätts centralt och i verksamheterna.

Svar på rekommendation 5: Kommunstyrelsen instämmer i revisorernas bedömning. På verksamhetsnivå kommer det enligt kommunstyrelsen under hösten 2019 att inledas en

samverkan med designerade informationssäkerhetsombud under ledning av trygghets- och säkerhetsavdelningen i syfte att skapa medvetande och involvering i stadens informationssäkerhetsarbete. Dessa ombud ska bistå sina verksamheter med verksamhetsnära stöd i informationssäkerhetsarbetet, framförallt vad gäller användningen av KLASSA på lokal nivå. De kommer också att bistå dataskyddsombudet i personuppgiftsärenden tillsammans med stadens systemförvaltare.

Uppföljning av vidtagna åtgärder per december 2021: Formaliserade utbildningsinitiativ har fattats och en konkret plan för grundutbildning av stadens samtliga medarbetare i informationssäkerhet och GDPR finns på plats. Utbildningen består av en lång serie treminuterslektioner som skickas via e-post. Utbildningarna kommer att driftsättas den 15 februari 2022. Beslutat organisatoriskt förslag som möter rekommendationen om designerade informationssäkerhetsroller saknas.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Bedömningen grundar vi på att formaliserade utbildningsinitiativ har tagits, men att designerade informationssäkerhetsroller saknas på respektive nämnd och styrelser i helägda bolag.

Rekommendation 6: Tillse att en utbildningsplan för informationssäkerhet formaliseras. Denna bör innefatta genomförande av obligatoriska och regelbundna utbildningar inom informationssäkerhet med uppföljning av deltagande. Kommunstyrelsen rekommenderas även tillse att kommunikation och signering av användaranvisningen för nyttjande av stadens IT-miljö säkerställs.

Svar på rekommendation 6: Kommunstyrelsen instämmer i revisorernas bedömning. Under 2019/2020 kommer enligt uppgift trygghets- och säkerhetsavdelningen att ta fram webbaserade kortutbildningar som stadens samtliga medarbetare ska erbjudas. I detta arbete ingår också att undersöka vilka möjligheter Sundbybergs stad har att knyta tillträdet till stadens IT-system för nyanställda till fullföljandet av obligatoriska webbutbildningar inom området informationssäkerhet.

Uppföljning av vidtagna åtgärder per december 2021: Vad gäller formaliserade utbildningsinitiativ, se svar på fråga 5 ovan. Det finns användaranvisningar för nyttjande av stadens IT-miljö (2021-04-08) som signeras av samtliga anställda, förtroendevalda och konsulter, men efterlevnaden av den följs inte upp. Det är inte klarlagt var ansvaret för en sådan uppföljning ligger.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Bedömningen grundar vi på att formaliserade utbildningsinitiativ har tagits. Vidare har kommunstyrelsen säkerställt användarvisningar för nyttjande av stadens IT-miljö som är obligatoriskt för samtliga anställda att signera. Kommunstyrelsen har inte kunnat redovisa hur efterlevnaden följs upp.

Rekommendation 7: Tillse att en stadsövergripande process för åtkomsthantering formaliseras, inklusive tydliga tilldelnings- och borttagningsförfaranden av behörigheter.

Svar på rekommendation 7: Nämnden ställer sig bakom ett gemensamt arbete med en

stadsövergripande process för åtkomsthantering som även inkluderar periodiska genomgångar. Nämnden beskriver att användar- och behörighetshantering till stadens IT-miljö i dagsläget är standardiserad. Information hämtas automatiskt dagligen från personalsystemet, vilket medför att användarkonton är ständigt är uppdaterade under förutsättning att rätt information finns i personalsystemet. Ansvaret för verksamhetssystem ligger enligt stadens systemförvaltarmodell på verksamheterna. I många fall sker tilldelning och borttagning manuellt direkt i verksamhetssystemen. Nämnden anser att en gemensam process tillsammans med en matris kopplad till kritiska IT-system skulle höja IT-säkerheten i staden.

Uppföljning av vidtagna åtgärder per december 2021: Enligt stadens systemförvaltningsmodell (senast ändrad 2019-10-04) ansvarar systemförvaltarna för behörigheter i systemen. Hur detta sker är dock inte formulerat i en gemensam process. På övergripande nivå är behörigheter kopplade till användarkonto som i sin tur styrs av personalsystemet. Varje månad sker en s.k. kostnadskontroll, vilket startar med att löneenheten uppmanar alla chefer att i stadens personalsystem kontrollera sina respektive "grupper" så att rätt person finns på löne- och personallistan. Någon rensning av systemet sker inte, utan personen inaktiveras då det måste finnas en spårbarhet. Vid rekrytering och anställningsintervjuer ska rekryterande chef kontrollera ID på den personen som ska intervjuas. Vid ny uppläggning i HR-systemet sker personnummerkontroll mot Skatteverkets databas. Användarkonton uppdateras löpande under förutsättning att rätt information finns i personalsystemet.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats. Bedömningen grundar vi på att en stadsövergripande process för åtkomsthantering inte har formaliserats, då tydliga tilldelnings- och borttagningsförfaranden av behörigheter inte finns. Vi rekommenderar kommunstyrelsen att uppdatera systemförvaltningsmodellen och beakta ovan nämnda brister.

Rekommendation 8: Tillse att stadsövergripande kontroller utformas för standardisering av genomförande av periodiska genomgångar. Kommunstyrelsen rekommenderas också tillse att förteckningar eller matriser skapas kring vilka behörigheter som inte är lämpliga att kombinera inom och mellan kritiska IT-system.

Svar på rekommendation 8: Se svar på rekommendation 7.

Uppföljning av vidtagna åtgärder per december 2021: I de fall tilldelning och borttagning sker manuellt direkt i verksamhetssystemet kan brister finnas svarar kommunstyrelsen. Vidare saknas en gemensam process tillsammans med en matris kopplat till IT-system.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats.

Rekommendation 9: Tillse att ett tydligt processflöde för hantering av kritiska incidenter, inklusive roller, ansvar och rapporteringskrav, definieras som del av stadens incidenthanteringsprocess.

Svar på rekommendation 9: Nämnden delar revisorernas bedömning att tydligheten kring

incidentrapportering behöver öka. I dag skrivs IT- incidentrapporter och större IT-incidenter rapporteras till Myndigheten för samhällsskydd- och beredskap (MSB). Som en del av stadens övriga incidenthanteringsprocess ska processflödet för hantering av kritiska incidenter, inklusive roller, ansvar och rapporteringskrav gemensamt definieras och tydliggöras.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen svarar att avsaknaden av ett kommunicerat ledningssystem för informationssäkerhet gör att rekommendationen inte är uppfylld.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats.

Rekommendation 10: Tillse att en stadsövergripande process för hantering av programförändringar formaliseras, inklusive kontroller för säkerställande av ändamålsenlig ansvarsfördelning i införandet av programförändringar.

Svar på rekommendation 10: Nämnden instämmer i revisorernas bedömning och har därför redan påbörjat arbetet med en formaliserad process gällande hantering av programförändring. Processen har också utökats till att även gälla ändringar i såväl system som stadens IT-miljö som helhet, en så kallad ändringsprocess.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen uppger att en ändringsprocess är framtagen. Ändringsprocessen förklaras i detalj, däribland registrering, granskning, planering, beslut om standard/normal ändring, test, ändringsråd, utförande, uppföljning och avslut.

Vår bedömning: Vi bedömer att rekommendationen *har* beaktats.

Rekommendation 11: Tillse att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till stadens användare med en bestämd frekvens.

Svar på rekommendation 11: Kommunstyrelsen delar revisorernas bedömning, men lägger också till att det dock inte är sannolikt att periodiskt återkommande utskick når igenom informationsbruset och leder till förhöjd kunskap eller medvetenhet om informationssäkerheten. Stadsledningskontoret ser enligt uppgift därför över olika möjligheter att förbättra informationen kring olika policys, riktlinjer och rutiner av liknande dignitet som informationssäkerhetspolicyn. Det kan handla om riktade informationsinsatser till ansvariga, information vid rekrytering och vid olika förändringar i rutiner och motsvarande. Det finns också stora möjligheter att anhängiggöra informationen i samband med närbesläktad informationsspridning. Det kan också finnas möjligheter att bifoga information i de digitala verktyg och system som används för dokument- och informationshantering.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen svarar att informationssäkerhetsrelaterad information bland annat kommuniceras via arbetsplatsträffar, medarbetarsamtal, intranät, nyhetsbrev till stadens alla chefer. Stadens lärplattform med ett antal webbaserade kurser kan också användas vid behov för

att exempelvis pusha ut information eller kunskapsprov. Vid nyanställning skrivs anvisningar för användning av stadens IT-miljö under i samband med att Multifunktionskort upprättas och lämnats ut.

Vår bedömning: Vi bedömer att rekommendationen *har* beaktats. Informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till stadens användare med en bestämd frekvens.

Rekommendation 12: Tillse att kontinuitetsplaner utformas för samtliga verksamhetssystem som i genomförd informationsklassning har bedömts som skyddsvärda, samt att samtliga kontinuitetsplaner samlas ihop på Stadsledningskontorsnivå för central kvalitetssäkring och koordinering av regelbunden testning av kontinuitetsplanerna.

Svar på rekommendation 12: Kommunstyrelsen instämmer i revisorernas bedömning och skriver att trygghets- och säkerhetsavdelningen under försommaren 2019 under ledning av enheten för digitalisering och service har inlett ett arbete med att identifiera stadens kritiska verksamhetssystem. När modellen för att identifiera dessa är fastställd ska samtliga identifierade system grundligt informationsklassificeras och därefter ska det för varje system upprättas kontinuitetsplaner som löpande ska följas upp och testas.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen hänvisar till den egenutvecklade tjänsten systemkollen, där dokumentation av förekomst av system och kontinuitetsplaner har börjat användas. Systemkollen innehåller dock inte komplett information och saknar förvaltningsplan. Stadsmiljö- och tekniska nämndens förvaltningsavdelning för digitalisering och service genomför för närvarande en systeminventering. Vad gäller ansvar svarar stadsledningskontoret att respektive nämnd och bolagsstyrelse har ansvar för de verksamhetssystem som de är systemägare för. Därför ska inte kontinuitetsplaner samlas ihop, utan förvaras på respektive förvaltningsmyndighet eller aktiebolag.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Systemkollen har börjat användas men är under utveckling.

Rekommendation 13: Tillser att en fullständig registerförteckning upprättas.

Svar på rekommendation 13: Kommunstyrelsen instämmer i revisorernas bedömning och påtalar att registerförteckningen under 2020 kommer att omarbetas i samarbete med informationssäkerhetsombuden och systemförvaltarna i verksamheterna. Därefter ska förteckningen löpande uppdateras, dock som minst en gång årligen.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen svarar att en mall för registerförteckning finns upprättad och kan hämtas av personuppgiftsansvarig nämnd och styrelse i helägda bolag på stadens intranät. I mallen finns bland annat en förteckning över informationstillgångar och en förteckning över personuppgiftsbehandlingar. Vad gäller handlingsplaner hänvisas till föregående svar på rekommendation 12.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats. Kommunstyrelsen har inte kunnat visa hur man inom ramen för sitt uppföljningsansvar säkerställt att personuppgiftsansvariga nämnder och bolagsstyrelsen har en uppdaterad och giltig registerförteckning. Kommunstyrelsen har inte för egen del kunnat påvisa en aktuell registerförteckning.

2.2. Sammanfattande bedömning

Vad gäller granskningen av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering bedöms kommunstyrelsen sammanfattningsvis delvis ha beaktat revisorernas iakttagelser och rekommendationer, samt vidtagit relevanta åtgärder av lämnade rekommendationer. I några fall konstaterar vi att ett arbete pågår och en del rekommendationer därför inte har beaktats fullt ut. I flera fall har revisorernas rekommendationer varken beaktats eller åtgärdats, däribland kvarstår vissa brister som vi bedömer vara av allvarlig karaktär.

Bland kvarstående brister vill vi bland annat lyfta fram att vi anser det vara allvarligt att ett beslutat och kommunicerat ledningssystem för informationssäkerhet fortsatt saknas. Det är inte ett lagstadgat krav att implementera ett ledningssystem för informationssäkerhet, men det kan enligt vår bedömning dels betraktas som vedertagen praxis, dels ha en betydande inverkan på resterande delar i stadens informationssäkerhetsarbete. Resultatet är att Sundbybergs stad fortsatt saknar flertalet grundläggande komponenter för att säkerställa ändamålsenlig informationssäkerhetsstyrning, däribland en informationssäkerhetsspecifik organisationsstruktur, adekvata uppföljningar samt en formulerad stadsövergripande process för åtkomsthantering.

Vår sammanfattande bedömning är således att kommunstyrelsen inte har nått tillräckligt långt i arbetet vad gäller informationssäkerhet mot bakgrund av tidigare lämnade rekommendationer. Detta även fast relativt lång tid har förflutit sedan tidigare granskning. Det kvarstår därför ett omfattande arbete för att åtgärda de rekommendationer som delvis, alternativt inte, har beaktats.

3. Granskning av efterlevnad - Dataskyddsförordningen GDPR

Granskningens syfte var att ge en övergripande förståelse och bedöma huruvida Sundbybergs stad och dess helägda bolag bedriver ett ändamålsenligt arbete med dataskyddsförordningen GDPR och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar.

Utifrån EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter genomfördes en översiktlig granskning av 12 olika områden under november 2019 till februari 2020. Enligt metoden bedöms stadens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Analysen baserades på intervjuer med identifierade nyckelpersoner i stadens och dess helägda bolags personuppgiftssäkerhetsarbete samt genomgång av insamlad styrdokumentation i staden och bolagen.

Baserat på den genomförda analysen och granskningen bedömdes Sundbybergs stad ha en förhållandevis låg mognadsgrad på 1,9 av maximalt 5,0. Mognadsgraden bedömdes vara som högst inom incidenthantering samt begäran från och information till registrerade. Lägst bedömdes mognadsgraden vara inom styrning och riskhantering. De helägda bolagen bedömdes sammantaget ha medel till god mognadsgrad i förhållande till jämförbara organisationer, med undantag för vissa specifika områden inom respektive bolag.

Granskningen konstaterade att stadens mest väsentliga utvecklingsområde var att ta fram och anta fullständiga styrdokument på personuppgiftsområdet. Vidare bedömdes att staden även tydligt måste dokumentera organisationsstrukturen, främst avseende IT- och informationssäkerhetsbefattningar, med tydlig ansvarsfördelning, samt eventuellt revidera organisationsstrukturen. Organisationsstrukturen och brister i tilldelade resurser vid tiden för granskningen bedömdes ligga till grund för de problem som rapporten identifierar för Sundbybergs stad. Övriga väsentliga förbättringsområden gäller införande av regelbundna utbildningar, strukturerade granskningar med föreslagna åtgärder och en översyn av leverantörsrelationerna. Av de 12 områden EY granskat har staden komplett dokumentation endast för incidenthantering.

Utifrån granskningens resultat riktades följande fem rekommendationer till staden:

1. För att säkerställa att Sundbybergs stads alla bolags och verksamheters rutiner beträffande hantering av personuppgifter sker i enlighet med kraven i dataskyddsförordningen bör Sundbybergs stad förtydliga sin informationssäkerhetspolicy. Genom denna kan en strategi och ett förtydligat syfte för dataskyddsarbetet förankras från politisk nivå hela vägen ner i verksamheterna. Policyn hänvisar till riktlinjer och anvisningar för dataskyddsarbetet, men dessa saknas och bör således skapas. De bör täcka in alla relevanta aspekter av dataskyddsförordningen. Sundbybergs stad rekommenderas även implementera en rutin för att följa upp att verksamheterna efterföljer de regler och policys som är fastställda i styrdokumentet.
2. Sundbybergs stad bör dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning för att undvika överarbetsbelastning och personberoende. EY föreslår även att organisationsstrukturen ses över och eventuellt ändras till att bättre passa IT:s

centrala roll i stadens verksamheter och de ökade kraven på informationssäkerhet. Dessutom bör staden avsätta resurser specifikt för att utveckla sitt dataskyddsarbete, så att man kan utföra gap-analyser[3] av utvecklingsområden, skapa tillhörande rutiner och processer, och sedan granska efterlevnaden av de processer som implementerats. Sundbybergs stad rekommenderas följaktligen också att fastställa en åtgärdsplan inkluderande tidsplan och ansvarig person för att åtgärda eventuella gap där dataskyddsförordningen inte efterlevs.

3. Staden rekommenderas att implementera en granskningsplan för att utvärdera och säkerhetsställa att man uppfyller relevanta krav på hantering av personlig information samt en formell rutin för att dokumentera och rapportera resultat till ledningsnivå. Kontroller av stadens dataskyddsarbete kan exempelvis integreras i stadens och dess nämnders internkontrollarbete. Staden rekommenderas även att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen.
4. Staden rekommenderas att instruktioner och rutiner kring incidenthantering bör kommuniceras regelbundet. Staden bör se till att nyanställda genomför en utbildning inom alla relevanta aspekter av personuppgiftshanteringen och att alla medarbetare genomför utbildningar regelbundet, exempelvis en gång per år. Utbildningarna bör uppdateras alltjämt som lagkraven blir tydligare och nya exempel finns tillgängliga.
5. Staden rekommenderas att slutföra sin inventering av de IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer, samt att ingå PUB-avtal med samtliga leverantörer där det är relevant.

3.1. Uppföljning av vidtagna åtgärder

Nedan följer i tur och ordning rekommendation, tidigare lämnat svar på rekommendation i samband med granskningen, uppföljning av vidtagna åtgärder samt vår bedömning – dvs. hur väl rekommendationen har beaktats.

Rekommendation 1: För att säkerställa att Sundbybergs stads alla bolags och verksamheters rutiner beträffande hantering av personuppgifter sker i enlighet med kraven i dataskyddsförordningen bör Sundbybergs stad förtydliga sin informationssäkerhetspolicy. Genom denna kan en strategi och ett förtydligat syfte för dataskyddsarbetet förankras från politisk nivå hela vägen ner i verksamheterna. Policyn hänvisar till riktlinjer och anvisningar för dataskyddsarbetet, men dessa saknas och bör således skapas. De bör täcka in alla relevanta aspekter av dataskyddsförordningen. Sundbybergs stad rekommenderas även implementera en rutin för att följa upp att verksamheterna efterföljer de regler och policys som är fastställda i styrdokumentet.

Svar på rekommendation 1: Kommunstyrelsen instämmer i revisorernas bedömning gällande informationssäkerhetspolicyn. Ett förslag till ny informationssäkerhetspolicy togs fram i februari 2020 av stadsledningskontoret och inväntar vid svarstillfället godkännande för remissbehandling i stadens nämnder och bolag. Kommunstyrelsen fastställer därefter, i enlighet med bestämmelsen i dess reglemente om att leda arbetet med

[3] En gap-analys åsyftar en analys av nuläget av informationssäkerhetsarbetet. Uttrycket syftar på gapet mellan det som standarden beskriver som bästa praxis och den rådande säkerhetsnivån i verksamheten.

informationssäkerhet, dessa riktlinjer för staden. För att riktlinjerna ska kunna verkställas skriver kommunstyrelser att det krävs lokala rutiner och rutiner för uppföljning på central nivå. Nämnderna måste upprätta lokala rutiner utifrån verksamhetskännedom medan kommunstyrelsen tar fram rutiner för central uppföljning. För att kunna följa att egenkontroller genomförs i enlighet med de bestämmelser som framgår av dataskyddsförordningen bedöms det nödvändigt att införa ett verksamhetssystem i vilket nämnderna kan genomföra sina egenkontroller.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen svarar att den tillgängliga informationssäkerhetspolicyn inte är aktualitetsprövad sedan 2017. Kommunstyrelsens tidigare svar om att en ny informationssäkerhetspolicy är under framtagande kvarstår. Beslutade riktlinjer för informationssäkerhet saknas fortfarande. Vad gäller rekommendationen om att implementera en rutin för att följa upp att verksamheterna efterföljer de lagar, regler och policys som är fastställda i styrdokumentet hänvisar kommunstyrelsen till Sundbybergs stads styrmodell med principer för planering, uppföljning och ekonomistyrning som gäller från och med 1 januari 2018. Nämnder och styrelser i helägda bolag ska enligt styrmodellen arbeta med att identifiera kritiska kvalitetsfaktorer för att säkra grunduppdraget utifrån perspektiven målgrupp, verksamhet, medarbetare och ekonomi. För att kunna följa upp resultatet ska mätbara indikatorer för varje kvalitetsfaktor fastställas. Några kritiska kvalitetsfaktorer har inte fastställts som har bäring på informationssäkerhet och GDPR. Kommunstyrelsen bedömer dock att detta kan utvecklas tydligare i planeringsanvisningarna inför mål och budget eller att tydliggöra ett antal stadsövergripande kritiska kvalitetsfaktorer som ska finnas med i alla nämnders och styrelser i helägda bolag verksamhetsplaner. För kommande år finns inga specifika skrivningar om informationssäkerhet i Sundbybergs stads mål och budget 2022.

Vår bedömning: Vi bedömer att rekommendationen *inte* har beaktats. Bedömningen grundar sig på att informationssäkerhetspolicyn inte har aktualitetsprövats och att beslutade riktlinjer för informationssäkerhets saknas. I Sundbybergs stads styrmodell finns anvisningar om hur nämnder och styrelser i helägda bolag ska följa upp kritiska kvalitetsfaktorer. Några kritiska kvalitetsfaktorer utifrån de ovan beskrivna perspektiven där informationssäkerhet och GDPR bör inrymmas, har inte fastställts.

Rekommendation 2: Sundbybergs stad bör dokumentera en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning för att undvika överarbetsbelastning och personberoende. EY föreslår även att organisationsstrukturen ses över och eventuellt ändras till att bättre passa IT:s centrala roll i stadens verksamheter och de ökade kraven på informationssäkerhet. Dessutom bör staden avsätta resurser specifikt för att utveckla sitt dataskyddsarbete, så att man kan utföra gap-analyser av utvecklingsområden, skapa tillhörande rutiner och processer, och sedan granska efterlevnaden av de processer som implementerats. Sundbybergs stad rekommenderas följaktligen också att fastställa en åtgärdsplan inkluderande tidsplan och ansvarig person för att åtgärda eventuella gap där dataskyddsförordningen inte efterlevs.

Svar på rekommendation 2: Kommunstyrelsen instämmer i revisorernas bedömning. Kommunstyrelsen svarar att det under hösten 2019 inleddes en samverkan med utsedda

informationssäkerhetsombud under ledning av trygghets- och säkerhetsavdelningen i syfte att skapa medvetande och involvering i stadens informationssäkerhetsarbete. Dessa kommer också att bistå dataskyddsombudet i personuppgiftsärenden tillsammans med stadens systemförvaltare. Målet med åtgärden beskrivs vara att försöka lätta på den arbetsbelastning och det personberoende som revisorerna identifierat. Stadsledningskontoret har tagit fram en arbetsmodell för informationsklassificering som består av fyra steg: Omvärldsanalys, verksamhetsanalys, riskanalys och gapanalys. Dessa analyser bedöms enligt kommunstyrelsen gemensamt möta revisorernas rekommendation att utföra gapanalyser av olika utvecklingsområden. Gapanalyserna ska också redovisa tidplaner och ansvar för att åtgärda eventuella gap inom informationssäkerheten. Kommunstyrelsen uppger att arbetet förväntas bedrivas under en oöverskådlig tid framåt. En tidsbegränsning av uppdraget bedöms inte lämplig då det rör sig om omfattande informationsmaterial som ska analyseras och kommunstyrelsens bedömning är att det är prioriterat att arbetet görs grundligt.

Kommunstyrelsen konstaterar också att uppdragen som informationssäkerhetssamordnare och dataskyddsombud inte är lämpliga att kombinera. Som framgår av föreliggande granskning och av den granskning som genomfördes av informationssäkerhetsarbetet under 2019 skulle det behövas två informationssäkerhetsombud på ändamålsenlig omfattning för att möta alla de rekommendationer som stadens revisorer lämnat. I övrigt skulle dataskyddsombudet behöva vara en självständig resurs för att stötta staden i hela dataskyddet. På sikt, bör omfattningen av denna tjänst ses över, då personuppgiftsansvaret åligger respektive nämnd, inte dataskyddsombudet skriver kommunstyrelsen. Samtliga nämnder, inklusive kommunstyrelsen, behöver således axla ett större ansvar för personuppgiftsskyddet och det praktiska arbetet som följer av det ansvaret än de i dagsläget gör.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen har inte beslutat och implementerat en informationssäkerhetsspecifik organisationsstruktur. Däremot är rollerna mellan informationssäkerhetssamordnare och dataskyddsombud sedan juni 2021 separerade. Vad gäller rekommendationen om att fastställa en åtgärdsplan hänvisar kommunstyrelsen till dokumentet Handlingsplan informationssäkerhet 2022–2024. Där finns bland annat en gap-analys och en tidsplan för arbetet. Gap-analysen bygger på stadens klassningsmodell för informationsklassificering som finns i systemverktyget KLASSA som tillhandahålls via SKR.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Bedömningen grundar sig på att det ännu inte finns en informationssäkerhetsspecifik organisationsstruktur. Dock har rollerna mellan informationssäkerhetssamordnare och dataskyddsombud separerats, och en åtgärdsplan finns framtagen.

Rekommendation 3: Staden rekommenderas att implementera en granskningsplan för att utvärdera och säkerhetsställa att man uppfyller relevanta krav på hantering av personlig information samt en formell rutin för att dokumentera och rapportera resultat till ledningsnivå. Kontroller av stadens dataskyddsarbete kan exempelvis integreras i stadens och dess nämnders internkontrollarbete. Staden rekommenderas även att fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och

kommuniceras till ledningen.

Svar på rekommendation 3: Kommunstyrelsen instämmer i revisorernas bedömning. Varje nämnd har var för sig utsett dataskyddsombudet och enligt förordningen ska dataskyddsombudet regelbundet beredas tillgång till ledningen. En sådan tillgång i förordningens mening tar inte enbart sikte på tjänstemannaledningen utan också på nämnden eftersom den bär det yttersta personuppgiftsansvaret. I enlighet med dataskyddsförordningen är det också den personuppgiftsansvariges skyldighet att aktivt efterfråga information och avrapportering i nämnden, samt hålla sig uppdaterad om förvaltningens hantering av personuppgiftsrelaterad information. Enligt kommunstyrelsen ska stadsledningskontoret under 2020 ta fram rutiner för hur avrapportering till varje nämnd med regelbundenhet ska ske.

Vidare gör kommunstyrelsen ett förtydligande rörande rekommendationen att kommunstyrelsen också ska fastställa ett rapporteringskrav gällande frekvens och innehåll som rapporteringen till kommunstyrelse ska utgå från för att säkerställa att uppföljning av dataskyddsförordningen utförs och kommuniceras till ledningen. Vad revisionen avser torde vara att kommunstyrelsen ska ta fram en rutin för hur rapporteringen ska gå till. Den ska sedan användas av samtliga nämnder i deras verksamheter, inte enbart av kommunstyrelseförvaltningens egenrapportering. Syftet med rutinen är att säkra att kommunstyrelsen kan ta sitt ledningsansvar för dataskyddet i staden, men fråntar inte nämnderna skyldigheten att genomföra egenkontroller genom sitt utnämnda dataskyddsombud skriver kommunstyrelsen.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen hänvisar till svar som lämnats under rekommendation 1. Varje nämnd och bolagsstyrelse har enligt stadens styrmodell uppdrag att årligen, i samband med budgetarbetet, upprätta en risk- och väsentlighetsanalys samt internkontrollplan. Kommunstyrelsens generella bedömning är att detta kan utvecklas ytterligare vad gäller GDPR och informationssäkerhet. Dataskyddsombudet som är i personunion för nämnderna, har enligt sin självständiga ställning att löpande följa upp hur respektive personuppgiftsansvarig nämnd efterlever gällande rätt. Dataskyddsombudet ska enligt sin instruktion en gång per kalenderår avge en uppföljningsrapport till respektive personuppgiftsansvarig nämnd. Vidare ska dataskyddsombudet också upprätta en uppsiktsrapport till kommunstyrelsen där samtliga nämnder och bolagsstyrelserna i de helägda bolagens arbete ska följas upp. Kommunstyrelsen har med anledning av antagandet av Handlingsplan informationssäkerhet 2022–2024 även uppmärksammats på att medvetenheten hos respektive nämnd och styrelse i helägda bolag behöver öka ytterligare och föreslår därför kommunfullmäktige i "Förslag till kommunfullmäktige om att uppmana stadens nämnder och genom Sundbybergs stadshus AB anmoda stadens bolagsstyrelser",
att i den egna risk- och väsentlighetsanalysen för verksamhetsåren 2022–2024 uppta risken för att verksamheten röjer sekretessbelagda uppgifter i strid med Offentlighets- och sekretesslag (2009:400) samt risken för att personuppgifter överförs till tredje land i strid med Dataskyddsförordningen. De aktiviteter som upptas i Sundbybergs stads handlingsplan för informationssäkerhet 2022–2024 ska utgöra miniminivån av nämndernas och styrelsernas kontrollaktiviteter. Riskerna och åtgärderna ska ingå i nämndernas och bolagsstyrelsernas internkontrollplaner för samma tidsperiod som ovan.

Vår bedömning: Vi bedömer att rekommendationen *har* beaktats. Utifrån stadens

styrmodell finns rapporteringsstrukturer samt ett riskanalys/IKP-arbete som potentiellt kan inkorporera informationssäkerhet. Vidare har kommunstyrelsen även lämnat en skrivelse till kommunfullmäktige i syfte att stärka IKP till 2022. Dataskyddsombuden lämnar även rapporter enligt en regelbunden och fastställd frekvens.

Rekommendation 4: Staden rekommenderas att instruktioner och rutiner kring incidenthantering bör kommuniceras regelbundet. Staden bör se till att nyanställda genomför en utbildning inom alla relevanta aspekter av personuppgiftshanteringen och att alla medarbetare genomför utbildningar regelbundet, exempelvis en gång per år. Utbildningarna bör uppdateras alltjämt som lagkraven blir tydligare och nya exempel finns tillgängliga.

Svar på rekommendation 4: Kommunstyrelsen instämmer i revisorernas bedömning och skriver att stadsledningskontoret under 2020 kommer att ta fram webbaserade kortutbildningar som stadens samtliga medarbetare ska erbjudas. I detta arbete ingår också att undersöka vilka möjligheter Sundbybergs stad har neka tillträdde till stadens IT-system för nyanställda till fullföljandet av obligatoriska webbutbildningar inom området informationssäkerhet. Stadsledningskontoret ser också över möjligheten att i olika former koppla e-utbildningar till kvitteringen av inpasseringskort.

Uppföljning av vidtagna åtgärder per december 2021: Kommunstyrelsen hänvisar till uppföljande svar till rekommendation 6 och 11 vad gäller informationssäkerhet.

Vår bedömning: Vi bedömer att rekommendationen *har* beaktats. Instruktioner och rutiner kring informationssäkerhet och GDPR kommuniceras regelbundet. Formaliserade utbildningsinitiativ har tagits som driftsätts den 15 februari, däribland om relevanta aspekter av personuppgiftshantering.

Rekommendation 5: Staden rekommenderas att slutföra sin inventering av de IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer, samt att ingå PUB-avtal med samtliga leverantörer där det är relevant.

Svar på rekommendation 5: Kommunstyrelsen instämmer i revisorernas bedömning. Stadsledningskontoret har sedan våren 2019 enligt kommunstyrelsen samverkat med samhällsbyggnads- och serviceförvaltningen kring ett arbete med att identifiera samtliga verksamhetskritiska IT-system. Det i kombination med att hela staden nu genomför en uppdatering av registerförteckningen syftar till att skapa en fullständig förteckning över alla driftsatta och aktiva verksamhetssystem i staden, inkluderat fullständig kontroll över den personuppgiftsbehandling som där förekommer. Under 2020 ska en fördjupad kontroll över stadens personuppgiftsbiträdesavtal genomföras med tonvikt på att upprätta sådana avtal där det i dagsläget eventuellt saknas uppger kommunstyrelsen.

Uppföljning av vidtagna åtgärder per december: Kommunstyrelsen svarar att kommunfullmäktige har delegerat personuppgiftsansvaret i reglementena till respektive nämnd/styrelse. Personuppgiftsansvar nämnd/styrelse är skyldiga enligt dataskyddsförordningen att föra register enligt dataartikel 30. Personuppgiftsansvarig nämnd/styrelse ska upprätta avtal enligt artikel 28.3. Personuppgiftsansvarig

nämnd/styrelse kan via intranätet ladda ner ett stadsövergripande avtal för PUB-avtal. Personuppgiftsansvariga nämnd/styrelse kan via intranätet ladda ner en stadsövergripande och kvalitetssäkrad registerförteckning.

Vår bedömning: Vi bedömer att rekommendationen *delvis* har beaktats. Personuppgiftsansvaret åligger nämnderna och KS ansvar inryms huvudsakligen under uppsiktsplikten. Givet detta noterar vi att det finns en avtalsmall samt mall för registerförteckning på plats, men att det däremot saknas en stadsövergripande uppföljning av kommunstyrelsen och hur väl nämnderna och bolagsstyrelserna för register och ingår PUB-avtal med relevanta leverantörer.

3.2. Sammanfattande bedömning

Vad gäller granskningen av efterlevnaden av dataskyddsfördordningen GDPR bedöms kommunstyrelsen sammanfattningsvis delvis ha beaktat revisorernas iakttagelser och rekommendationer, samt vidtagit relevanta åtgärder av lämnade rekommendationer. I två fall konstaterar vi att ett arbete pågår och att en del rekommendationer därför inte har beaktats fullt ut. I ett fall har revisorernas rekommendationer varken beaktats eller åtgärdats. Vissa kvarstående brister bedömer vi vara av allvarlig karaktär.

Bland kvarstående brister vill vi bland annat lyfta fram att vi anser det vara allvarligt att informationssäkerhetspolicyn inte har aktualitetsprövats sedan 2017 och att beslutade riktlinjer för informationssäkerhet saknas. Vidare har inte heller några kritiska kvalitetsfaktorer utifrån informationssäkerhet och GDPR fastställts i linje med vad som anges i Sundbybergs stads styrmodell. Det saknas dessutom en stadsövergripande uppföljning av kommunstyrelsen och hur väl nämnderna och bolagsstyrelserna för register och ingår PUB-avtal med relevanta leverantörer.

Vår sammanfattande bedömning är således att kommunstyrelsen inte har nått tillräckligt långt i arbetet vad gäller GDPR mot bakgrund av tidigare lämnade rekommendationer. Detta även fast relativt lång tid har förflutit sedan tidigare granskning. Det kvarstår därför ett arbete för att åtgärda de rekommendationer som delvis, alternativt inte, har beaktats.

4. Uppföljning av stadens åtgärder med anledning av Schrems II (C311/18) "Överföring av personuppgifter till tredjeland"

EU-domstolen meddelade den 16 juli 2020 dom i mål C-311/18, det så kallade Schrems II-målet. Domen innebär i korthet att det har blivit olagligt att använda IT-baserade tjänster som på något sätt för över och behandlar personuppgifter i USA med stöd i regelverket kallad Privacy Shield.

I Sundbybergs stad används amerikanska molntjänster i stora delar av verksamheten. Kommunstyrelsen kom efter genomförd övergripande risk- och sårbarhetsanalys fram till följande ställningstagande:

"Att med omedelbar verkan avbryta användandet av verksamhetskritiska molntjänster där det finns risk att tredje land får tillgång till personuppgifter bedöms inte möjligt att genomföra utan att bryta mot det uppdrag kommunen har enligt kommunallagen, generella lagstiftningar och speciallagstiftningar.

Detta grundar sig på att konsekvenserna av ett omedelbart stopp medför högre risker än att acceptera de risker som uppkommer genom ett fortsatt användande under den tid det tar att hantera riskerna. Inga nya avtal ska tecknas med leverantörer som erbjuder tjänster där det finns risk för överföring av personuppgifter till tredje land. Åtgärder för att hantera befintliga brister behöver påbörjas omgående."

Denna granskning omfattar även uppföljning av stadens åtgärder med anledning av Schrems II (C311/18) "Överföring av personuppgifter till tredjeland". Mot bakgrund av ovan beskrivna ställningstagande har kommunstyrelsen gjort en utredning som beskriver vad Schrems II-domen kan innebära för staden samt förslag till hantering av tjänster att överföra personuppgifter till tredje land. Nedan presenteras kommunstyrelsens förslag (2021-10-06) på hur staden ska gå vidare.

Steg 1
Det första steget föreslås vara att respektive nämnd / bolagsstyrelse tillser att de har kontroll över

- vilka personuppgiftsbehandlingar nämnden /bolagsstyrelsen har,
- vem som äger dessa behandlingar,
- vilka av dessa behandlingar som har, respektive saknar, giltiga avtal som reglerar GDPR-efterlevnad (personuppgiftsbiträdesavtal),
- vilka de molntjänster är där det finns risk för att personuppgifter förs över till tredje land,
- vilka verksamhetskritiska informationsbehandlingar som har, respektive saknar, kontinuitetsplan.

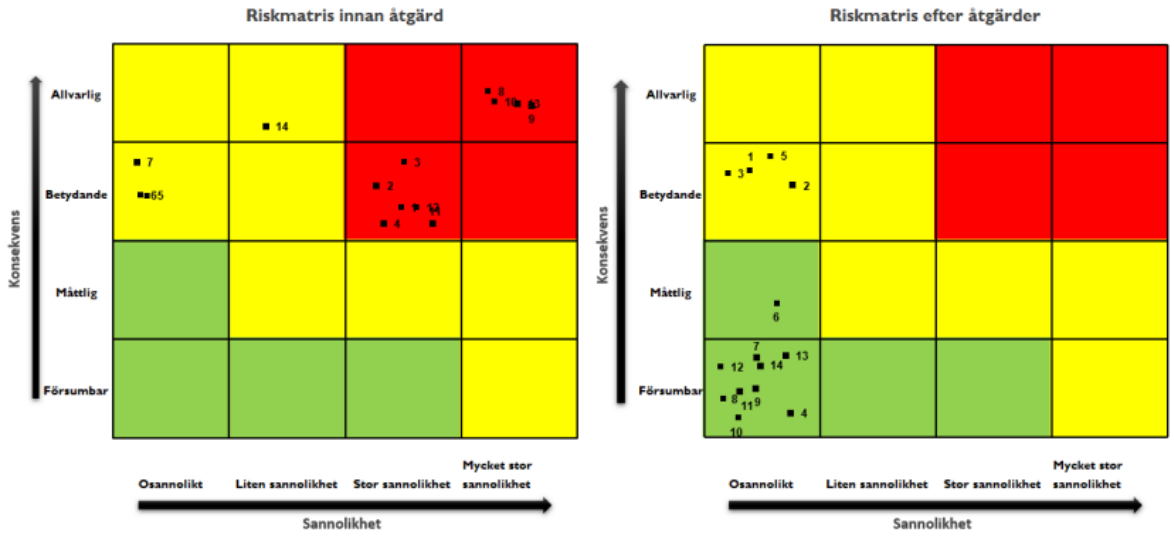
Detta ska redan finnas noterat i nämndens / bolagsstyrelsens registerförteckningar, som ska föras enligt GDPR. Om det inte finns ska det åtgärdas snarast. Mall för registerförteckning tillhandahålls av kommunstyrelsen.

Steg 2
Steg två föreslås vara att respektive nämnd/bolagsstyrelse

- tillser att gällande personuppgiftsbiträdesavtal finns för samtliga personuppgiftsbehandlingar.
- tillser att kontinuitetsplan upprättas för verksamhetskritiska informationsbehandlingar

- låter genomföra egen risk- och sårbarhetsanalys för i första hand verksamhetsåren 2022-2024. Analysen ska behandla användandet av molntjänster där risk finns för att verksamheten röjer sekretessbelagda uppgifter i strid med Offentlighets- och sekretesslag (2009:400) och / eller risk finns för att personuppgifter överförs till tredje land i strid med Dataskyddsförordningen. Med utgångspunkt i analysresultatet tas åtgärdsplaner fram för
    - införandet av administrativa åtgärder, dvs förändring i rutiner och arbetssätt i de tjänster det berör, för att så långt det är möjligt avstå från att hantera personuppgifter i strid med GDPR. Åtgärdsplanen föreslås vara framtagen senast den 30 juni 2022 och genomförd senast den 30 augusti 2022.
    - tillvägagångssätt och tidplan för att byta ut de it-tjänster som inte är förenliga med GDPR. En sådan åtgärdsplan föreslås vara framtagen senast den 31 januari 2023.

Steg 3
Steg tre ska vara att respektive nämnd/bolagsstyrelse vid behov genomför åtgärdsplan för byte av it-tjänst. Då utbyte av tekniska tjänster tar olika lång tid beroende på grad av komplexitet hänvisas tidplanen till att dokumenteras i respektive behandlings it-systems förvaltningsplaner. Ett åtgärdande av riskerna enligt denna strukturerade metod bedöms över tid kunna minska riskerna till en acceptabel nivå.



De risker som markerats som "betydande / osannolika" även efter åtgärder är inledande åtgärder som ska hanteras vidare i fortsatta åtgärder.

Uppföljning
Uppföljning av hantering av identifierade risker ingår i nämndernas och bolagsstyrelsernas internkontrollplan.

Vår bedömning: Kommunstyrelsen har med anledning av Schrems II-målet gjort en utredning avseende åtgärder vid användande av molntjänster. Utredningen landar i ett övergripande ställningstagande, samt i en väg framåt, uppdelad i tre steg. Vår bedömning är att utredningen förefaller vara gediget utförd, med analys av rätts- och omvärldsläget, samt ett övervägande av alternativa tjänster. Riskerna med att direkt avsluta ett stort antal tjänster vägs mot riskerna med att under en övergångsperiod fortsätta använda tjänsterna för att under ordnade former finna andra lösningar. Utredningens ställningstagande att inte omedelbart avsluta nuvarande tjänster, men att omgående vidta

åtgärder för att hantera befintliga risker, framstår som ändamålsenligt givet stadens utgångsläge, samt de generellt oklarheter som ännu finns kring effekterna av Schrems II. Ytterligare definiering av tidplan för åtgärder är inte känt vid tidpunkten för granskningen.

Bilaga 1 Källförteckning

Medverkande

- Säkerhetsskyddschef
- Avdelningschef för digitaliserings- och serviceavdelningen

Underlag

- Utredning avseende åtgärder för att säkerställa efterlevnad av GDPR vid användande av molntjänster i Sundbybergs stad
- Sundbybergs stads handlingsplan för informationssäkerhet 2022–2024 – beslut och remittering
- Handlingsplan för informationssäkerhet 2022–2024
- Övergripande risk- och sårbarhetsanalys – molntjänster
- Sundbybergs stads dataskyddsombudsskrivelse
- Orienterande samtal – kommunrevisionen
- Anvisningar för användning av Sundbybergs stads IT-miljö
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Byggnads- och tillståndsnämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Grundskole- och gymnasienämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Förskolenämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Kultur- och fritidsnämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Social- och arbetsmarknadsnämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Stadsmiljö- och tekniska nämnden
- Verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023, Äldrenämnden
- Kommunstyrelsens verksamhetsplan med budget och internkontrollplan 2021 med plan för 2022–2023
- Affärsplan Fastighets AB Förvaltaren
- HR informerar #3, #4, #5, #6, #7 2021
- Instruktion för dataskyddsombudet
- Lokalfastigheter i Sundbyberg AB – Affärsplan med budget 2021
- Mall för medarbetarsamtal/lönegrundande samtal
- Informationssäkerhetspolicy för Sundbybergs stad
- Praktisk hantering av beslutsfrågor rörande IT-säkerhet
- Sundbybergs stads program för krisberedskap och civilt försvar
- Ändringsprocessen i detalj
- Sundbybergs stads styrmodell med principer för planering, uppföljning och ekonomistyrning
- Sundbybergs stads budget 2021 med plan 2022-2023
- Sundbybergs Stadsnäts verksamhetsplan 2021 med plan 2022–2023
- Systemförvaltningsmodell
- Sundbybergs stads budget med plan 2023-2028
- Vägledning för lagring
- Vårt medarbetarskap och ledarskap
- Registerförteckning – Personuppgiftsbehandlingar mall
- Vägledning – Att införa ett nytt verksamhetssystem