Revisionsrapport 2017
Genomförd på uppdrag av revisorerna
September 2017

Sundbybergs stad

Förstudie - granskning av förberedelse inför implementering av nya dataskyddsreformen

Building a better working world

Innehåll

1. Inledning 2

1.1. Bakgrund 2
1.2. Syfte och revisionsfrågor 2
1.3. Genomförande 2

2. Kommunkoncernens organisation för personuppgiftsfrågor 2

2.1. Stadens organisation 2
2.2. Bolagens organisation 3
2.3. Styrning och kompetens i staden 3

3. Implementeringsarbetet av GDPR 4

3.1. Tidigare iakttagelser i granskning rörande digitalisering av stadens verksamheter 4
3.2. Roll- och ansvarsfördelning 4
3.3. Finansiering 4
3.4. Dokumentation 5
3.5. Fortsatta arbetet och nästa fas 5

4. Sammanfattande bedömning 6

Källförteckning 7

1. Inledning

1.1. Bakgrund

Europeiska unionen (EU) beslutade i april 2016 om ett nytt regelverk (allmänna dataskyddsförordningen) för behandling av personuppgifter, som ska börja tillämpas av medlemsstaterna den 25 maj 2018. Regelverket benämns ”allmänna dataskyddsförordningen” (engelska förkortningen GDPR[1]). I denna rapport används fortsatt GDPR som benämning. GDPR kommer att, i jämförelse med personuppgiftslagen (1998:204), stärka den enskilda personens rättighet över sina personuppgifter och ställa strängare krav på bland annat myndigheter att informera om hur de hanterar enskildas personuppgifter. Det betyder att kommuner, landsting och regioner snabbt behöver inleda anpassningsarbetet till de nya reglerna. Avsteg eller överträdelser från GDPR kan innebära betydande sanktionsavgifter.

Det är av väsentlig betydelse att förberedelserna för det nya regelverket följer en tydlig och transparent struktur samt att kontinuerlig uppföljning sker på ett ändamålsenligt sätt. Vidare är det av väsentlig betydelse att ändamålsenlig kompetens finns att tillgå inom den organisation som ska anpassa sig till det nya regelverket. Efter genomförd förstudie beslutar stadens revisorer huruvida det finns behov av en fördjupande granskning.

1.2. Syfte och revisionsfrågor

Syftet med förstudien är att inhämta information om stadens arbete med att förbereda sig för den nya dataskyddsförordningen, vad gäller roller- och ansvar, tillgång till resurser och kompetens samt huruvida ändamålsenlig tidplan föreligger.

1.3. Genomförande

Förstudien grundas på dokumentstudier (se bilaga 1) och intervjuer med enhetschef för kommunsekretariat och arkiv. Intervjuade har beretts tillfälle att sakgranska rapporten. Granskningen är genomförd juni-september.

2. Kommunkoncernens organisation för personuppgiftsfrågor

2.1. Stadens organisation

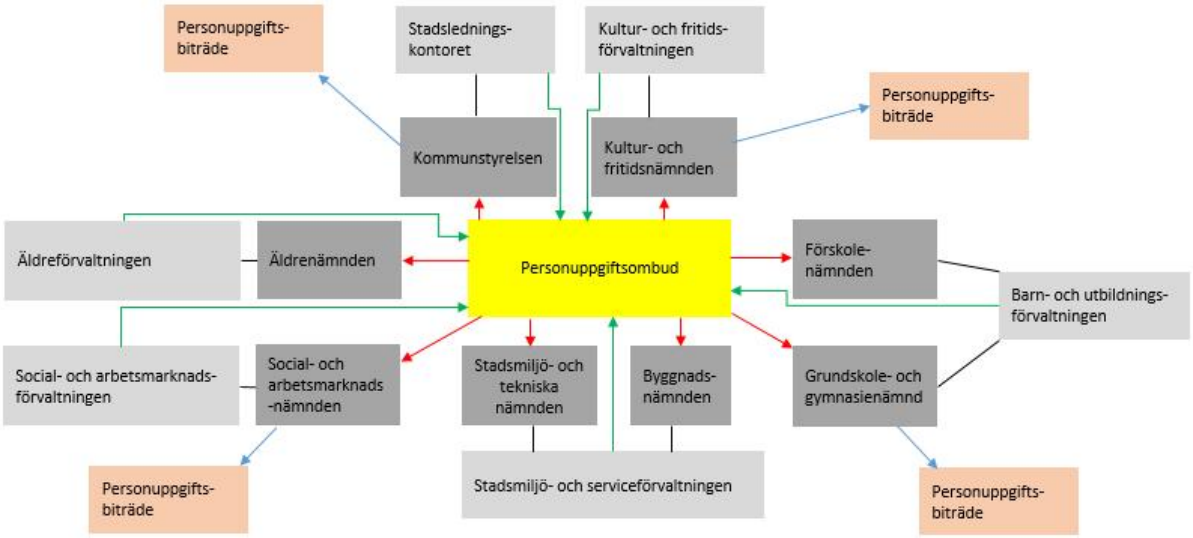
Nedanstående figur illustrerar att nämnderna är personuppgiftsansvariga. Enligt personuppgiftslagens 3 § ”bestämmer de enskilt eller tillsammans med andra ändamålen och medlen för behandlingen[2] av personuppgifter”. De personuppgiftsansvariga har förordnat överförmyndarchefen till deras personuppgiftsombud, som enligt 3 § självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt i stadens verksamheter. Personuppgiftsombudet ska påpeka fel och brister till den personuppgiftsansvarige (se röda pilar). Beteckningen personuppgiftsombud ersätts i GDPR med dataskyddsombud, som kommuner kommer att vara skyldiga att utse. Ombudets roll blir att kontrollera att GDPR följs inom organisationen genom att utföra exempelvis kontroller men också informera om

[1] General Data Protection Regulation
[2] Varje åtgärd eller serie av åtgärder (t.ex. insamling, registrering, lagring, bearbetning och spridning) som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte.

förordningen. Därtill ska ombudet vara kontaktytan mot datainspektionen och samarbeta med denna.

I och med att staden utsett ett personuppgiftsombud ska verksamheten anmäla behandlingar av personuppgifter till personuppgiftsombudet (se gröna pilar). Personuppgiftsombudet ska föra en förteckning över anmälda behandlingar och dataregister. Personuppgiftsbiträden är exempelvis systemleverantörer eller andra externa parter som behandlar personuppgifter för den personuppgiftsansvariges räkning (se blåa pilar).

Figur 1 – Illustration av stadens personuppgiftsansvariga, personuppgiftsombud och personuppgiftsbiträden



(Figuren är EY:s egna)

2.2. Bolagens organisation

Enligt uppgift från stadens bolagsjurist har samtliga bolag med undantag för Sundbybergs stadshus infrastruktur AB utsett personuppgiftsombud.

2.3. Styrning och kompetens i staden

Av stadens egen förstudie, som genomfördes under våren 2017 (beskrivs närmare i avsnitt 3,4) framgår att nämnderna/personuppgiftsansvariga saknar generella styrinstrument såsom policy, riktlinjer och rutiner för behandling av personuppgifter. Istället sker arbetet på informell basis baserad på kompetenser och initiativ hos enstaka individer. I stadens förstudie bedöms det finnas en fungerande arbetsgång för anmälan av nya behandlingar av personuppgifter till stadens personuppgiftsombud.

Av förstudien framgår att bolagen saknar en styrning och styrdokument för behandling av personuppgifter. Det finns ett utkast till förteckning över personuppgiftsbehandlingar, men ambitionen att slutföra den har inte funnits i tillräcklig omfattning.

3. Implementeringsarbetet av GDPR

3.1. Tidigare iakttagelser i granskning rörande digitalisering av stadens verksamheter

I granskningen (rapporterades till revisionen i november 2016) framkom att det hade inletts ett informellt arbete med att förbereda staden inför införandet av GDPR. För arbetet hade tf. chef för administrations- och utvecklingsenheten tillika stadens personuppgiftsombud format en grupp bestående av informationssäkerhetssamordnaren, systemförvaltare på stadsledningskontoret och infrastrukturansvarige inom IT. Vidare framkom att arbetet skulle utgå ifrån datainspektionens vägledning till personuppgiftsansvariga. Arbetsgruppen hade, när granskningen genomfördes, bearbetat information och bokat in sig på länsstyrelsens seminariedag om GDPR. Under november 2016 skulle arbetsgruppen träffas i syfte att planera och fördela arbetsuppgifter.

3.2. Roll- och ansvarsfördelning

I samband med att intervjuad chef för kommunsekretariat och arkiv påbörjade sin anställning ”ärvde” denne ägarskapet för implementeringsarbetet av GDPR. En styrgrupp har formats för att stärka styrningen av implementeringsarbetet. Utöver den intervjuade består styrgruppen av förvaltningschef för stadsmiljö- och serviceförvaltningen samt IT-chef och bolagsjurist i Sundbybergs stadshus AB. Under våren har gruppen träffats tre gånger för planering av det fortsatta arbetet.

I dagsläget har inget formellt beslut fattats vilken nämnd som ska ansvara för dataskyddsfrågor. Den intervjuade anser att dataskyddsfrågor bör ligga under kommunstyrelsen. Då särskiljs granskning från utveckling, vilket det inte gjort om frågorna sorterats med övrig IT under stadsmiljö- och tekniska nämnden.

3.3. Finansiering

Enligt uppgift från den intervjuade finns i budget 200 tkr öronmärkt för implementeringsprojektet. Den tidigare kalkyleringen, som budgeten baseras på, har underskattat projektets omfattning och den intervjuade konstaterar att betydligt mer medel hade behövts öronmärkas. Verksamhetens anpassning till GDPR kan enligt den intervjuade hanteras med befintlig personal. Behovet av ytterligare medel rör arbete och anpassningar kopplade till IT-systemen.

Styrgruppen ser även ett framtida behov av att kommunkoncernen har två dataskyddsombud, ett för stadens verksamheter och ett för bolagen, som arbetar enbart med dataskyddsfrågor. Behovet får styra funktionernas omfattning och ett tänkbart upplägg kan vara att köpa tjänsten inledningsvis, för att sedan eventuellt anställa kompetens till kommunkoncernen, uppger den intervjuade.

Vår bedömning är att det föreligger en risk, som kan fordra finansiella medel, för eventuella juridiska tvister mellan staden och systemleverantör(er) rörande betalningsansvar för anpassning(ar) i IT-system(en).

3.4. Dokumentation

Vi har gått igenom kommunstyrelsens respektive stadsmiljö- och tekniska nämndens verksamhetsplan och intern kontrollplan för 2017. Genomgången visar att implementeringsarbetet inte finns upptaget i någon av verksamhetsplanerna. Implementeringsarbetet anges inte i risk- och väsentlighetsanalyser och ingår därmed inte i interna kontrollplaner. Bakgrunden till detta var dels förutsättningarna, dels bedömningen att takten i implementeringsarbetet behövde öka. Därtill prioriteringen av att genomföra en nulägesanalys. Risk- och väsentlighetsanalys kommer enligt uppgift att upprättas i nästa fas.

Vidare har vår genomgång av dessa två nämnders protokoll under perioden januari – augusti 2017 visat att ingen specifik information lämnats till nämnderna. Likt ovan kommer information och politiska inriktningsbeslut bli aktuella i nästa fas.

Under våren direktupphandlades Certezza (extern leverantör), för att leda ett projekt med målsättning att säkra att stadens nämnder och bolag lever upp till de krav som ställs på verksamheten i GDPR. Projektet ska inkludera framtagandet av en roadmap med nulägesanalys för stadens nämnder och stadens helägda bolag, samt en plan för arbetet fram till förordningen träder i kraft.

Projektet tillika förstudien anges ha bedrivits i totalt 11 workshops med deltagare från samtliga förvaltningar och bolag med undantag för Sundbyberg stadshus infrastruktur AB. Workshops med deltagare från de samägda bolagen[3] och kommunalförbunden[4] gjordes inte.

På workshoparna fick deltagarna en genomgång om GDPR och behandlingar av personuppgifter inventerades och dokumenterades. I stadens förstudie uppskattas det att det finns uppemot 200 behandlingar av personuppgifter inom koncernen. Siffran är dock en uppskattning och kan revideras vid en mera utförlig inventering. Huruvida behandlingarna förhåller sig till dataskyddsförordningens krav har inte kunnat analyseras inom förstudien.

Stadens förstudie gav ett antal rekommendationer som bland annat rör framtagande av styrdokument och rutiner, utvecklande av samarbetet med datainspektionen, utvecklande och dokumentering av personuppgiftsincidentrapportering och att utveckla upphandlings- och inköpsprocessen. Arbetet med rekommendationerna kommer att bli aktuellt i implementeringsarbetets nästa fas.

3.5. Fortsatta arbetet och nästa fas

Projektet tillika förstudien överlämnades till styrgruppen i juni. Härnäst kommer förstudien enligt den intervjuade att redovisas och förankras hos förvaltningschefer och VD:ar för bolagen. Därefter ska respektive förvaltning och bolag under hösten arbeta vidare med att anpassa verksamheten till GDPR. Samtidigt kommer styrgruppen prioritera och arbeta vidare med ovan beskrivna delar.

Enligt den intervjuade har styrgruppen gjort bedömningen att verksamheten ska ha relevant kunskap om GDPR när den träder i kraft. Därtill ha erfordrad dokumentation upprättad. Däremot bedöms implementeringsarbetet rörande IT-systemen ta tid och alla delar/frågor kommer inte vara färdiga/lösta till den 25 maj.

[3] Koncernen Norrenergi och miljö AB och Söderhalls renhållnings AB (Sörab) och AB Vårljus
[4] Norrvatten och Storstockholms brandförsvar

4. Sammanfattande bedömning

Vår sammanfattande bedömning är att staden har initierat ett arbete i syfte att uppfylla de krav som GDPR ställer från och med 2018. Dock är det vår uppfattning att omfattningen på det nödvändiga anpassningsarbetet till viss del har underskattats av staden. Vidare är vår bedömning att anpassningsarbetet som påbörjats har skett i ett sent skede, vilket innebär en risk att implementeringsarbetet inte kommer vara färdigt när förordningen träder i kraft 2018.

Med anledning av detta har revisionen dels för avsikt att nogsamt följa stadens, samt koncernbolagens, fortsatta arbete med anpassningar till GDPR, dels genomföra en fördjupad granskning i början av 2018.

Stockholm den 13 september 2017

Andreas Halvarsson
Verksamhetsrevisor

Källförteckning

Förfrågningsunderlag – Direktupphandling för konsultstöd kring dataskyddsdirektivet (GDPR) (daterat 2017-02-22)

Förstudie, efterlevnad Dataskyddsförordningen med tillhörande bilagor (daterad 2017-06-28)

Sundbybergs stads budget 2018 med plan för 2019-2020

Kommunstyrelsens verksamhetsplan för 2017

Kommunstyrelsens intern kontrollplan för 2017

Stadsmiljö- och tekniska nämndens verksamhetsplan för 2017

Stadsmiljö- och tekniska nämndens intern kontrollplan för 2017

Kommunstyrelsens sammanträdesprotokoll
2017-02-06
2017-03-13
2017-04-10
2017-05-15
2017-06-12
2017-06-26
2017-08-21

Stadsmiljö- och tekniska nämndens protokoll
2017-01-31
2017-02-21
2017-03-21
2017-04-25
2017-05-23
2017-06-20
2017-08-29