Uppföljande granskning av Informationssäkerhet

Stadsrevisionen. Borås

Kortrapport

2021-02-08

2021

Inledning

Stadsrevisionen genomförde 2017 en granskning av Borås Stads informationssäkerhet. Stadsrevisionen konstaterade att den interna kontrollen avseende informationssäkerheten inte var tillräcklig. De brister som identifierades bedömdes främst bero på att Borås Stad till stor del saknade uppdaterade policys och rutiner för informationssäkerhet. De dokument som fanns hade i flertalet fall inte beslutats i enlighet med delegationsordningen. Borås Stad saknade tillfredsställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantörer att ta del av uppgifter som Borås Stad gjorde tillgängliga via säkerhetskopiering. Kommunstyrelsen och berörda nämnder bedömdes behöva säkerställa att samtliga avtal som reglerar hanteringen av sekretessbelagda uppgifter var förenliga med offentlighets- och sekretesslagen.

Den 25 maj 2018 trädde EU:s nya dataskyddsförordning (DSF), mer känd som GDPR, i kraft. Den nya lagen ersätter den tidigare personuppgiftslagen (PUL) och gäller i alla EU-länder. Införandet av GDPR innebär bland annat ett förändrat regelverk kring hur organisationer lagrar och hanterar enskilda individers personuppgifter.

Syfte och frågeställningar

Syftet med granskningen är tvådelat, dels att genomföra en uppföljning av tidigare granskning från 2017 av informationssäkerhet, dels att granska hur Borås Stad har implementerat GDPR och NIS-direktivet.

Huvudsakliga frågeställningar är:

- Vilka styrdokument och planer har Borås Stad inom området?
- Hur har arbetet för att säkerställa förutsättningar för god informationssäkerhet utvecklats sedan 2017?
- Säkerställer Kommunstyrelsen en tillräcklig intern kontroll avseende den övergripande informationssäkerheten?
- Hur har Kommunstyrelsen bedrivit arbetet med att implementera GDPR och NIS-direktivet?

Granskningen avgränsas till att omfatta Borås Stads övergripande informationssäkerhetsarbete, arbete med att implementera GDPR och NIS-direktivet.

Revisionskriterier är Kommunallagen, Tryckfrihetsförordningen, Offentlighets- och sekretesslagen, Arkivförordningen, Arkivlagen och övrig tillämplig lagstiftning. Revisionskriterier är även Dataskyddsförordningen, NIS-direktivet samt rekommendationer från Integritetsskyddsmyndigheten (IMY, tidigare Datainspektionen) och Myndigheten för samhällsskydd och beredskap (MSB).

Bakgrund

Informationshantering

Med informationshantering avses de åtgärder som vidtas för att informationen ska kunna användas på ett ändamålsenligt och kontrollerat vis, genom att den skapas, struktureras, hanteras, förvaras och lagras på lämpligt sätt. Det kräver styrning och kontroll av informationen under hela dess livscykel, från klassificering, registrering, kvalitetssäkring, redovisning, tillgänglighet och värdering till skydd och förvaring, vilket även innefattar informationssäkerhetsfrågor.[1]

De regler och lagar som reglerar informationshanteringen är Tryckfrihetsförordningen, Offentlighet och sekretesslagen, Arkivlagen och arkivförordningen samt GDPR och andra speciallagar.

Borås har också lokala riktlinjer för informationshanteringen i form av arkivregler, rutiner för information- och arkivhantering, dokumenthanteringsplaner med råd och anvisningar samt egna rutiner eller lathundar som respektive förvaltning tagit fram.

Informationssäkerhet

Informationssäkerhet handlar om att skydda all känslig information oavsett i hur den uppkommer eller den lagras. Eftersom informationen i allt högre utsträckning finns i IT-system handlar informationssäkerhet i allt högre utsträckning om datatekniska lösningar.

Borås Stad med dess bolag hanterar en betydande del av samhällsservicen. Bolagens IT-service är skild från koncernen i övrigt. Det finns därför ingen sammanhållen bild över hela kommunkoncernens informationssäkerhet.

Utöver de lagar, riktlinjer och rutiner som finns för informationshanteringen i Borås Stad finns även specifika informationssäkerhetsrutiner för olika program. Stadsledningskansliet håller också på att ta fram en informationssäkerhetspolicy.

[1] Borås Stad – Informationshantering och arkiv https://intranet.boras.se/styrningochledning/handbockermetodermodellerochrutiner/offentligforvaltning/informationshanteringocharkiv.4.613655ff148a1209d2d49f31.html

Kommunallagen

Enligt 6 kap. 7 § Kommunallagen skall nämnderna var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de föreskrifter som gäller för verksamheten. De ska också se till att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Tryckfrihetsförordningen

Genom tryckfrihetsförordningen (1949:105) (TF) ges allmänheten rätt att ta del av allmänna handlingar (offentlighetsprincipen). En handling anses enligt 2 kap. § 4 TF som allmän om den är att anse som inkommen eller upprättad hos en myndighet.

Offentlighet- och sekretesslagen

Undantag från rätten att ta del av allmänna handlingar regleras i offentlighets- och sekretesslagen (2009:400) (OSL). Lagen innehåller även bestämmelser för registrering av allmänna handlingar.

Enligt 3 kap. 1 § OSL innebär sekretess ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Vid kontraktering som medför att informationen hos myndighet blir tillgänglig även för tjänsteleverantör måste begränsningar enligt OSL beaktas, och bedömning ske om överlämnandet är förenligt med OSL.

Arkivlagen – Arkivförordningen

Arkivlagen (1990:782) och arkivförordningen (1991:446) gäller för statliga och kommunala myndigheter. Den är även tillämplig på bolag, föreningar och stiftelser där kommunen utövar ett rättsligt bestämmande inflytande enligt 2 kap. 3 § OSL. I arkivlagen och arkivförordningen regleras ansvaret för de allmänna handlingarna och hur dessa får hanteras. Varje myndighet ansvarar för sina handlingar.

Ledningssystem för informationssäkerhet

Standarderna i ISO 27 000-serien har beteckningen Ledningssystem för informationssäkerhet och bildar grunden för att bedriva ett systematiskt informationssäkerhetsarbete i en organisation. Standarderna i ISO 27 000-serien är framtagna av internationella expertgrupper inom ISO/IEC (International Organisation for Standardization/International Electrotechnical Commission) där Sverige medverkar genom SIS (Swedish Standards Institute).[2]

[2] Informationssäkerhet.se Ledningssystem för informationssäkerhet https://www.informationssakerhet.se/stod--vagledning/standarder-for-informationssakerhet/ledningssystem-for-informationssakerhet/

MSB:s föreskrifter och allmänna råd och kommuners risk- och sårbarhetsanalyser

MSB:s föreskrifter om kommuners risk- och sårbarhetsanalyser (MSBFS 2015:5) innehåller indikatorer för bedömning av kommuners generella krisberedskap. Gällande informationssäkerhet menar MSB att kommunen hanterar information säkert genom att:[3]

- bedriva ett systematiskt arbete med informationssäkerhet i enlighet med tillämplig informationssäkerhetsstandard (ISO/IEC 27 001, ISO/IEC 27002) på området,
- ha rutiner för att identifiera och hantera kritiska beroenden till system och tjänster för informationshantering som är av central betydelse för kommunens verksamhet, samt
- ha rutiner för att identifiera och hantera säkerhetsbrister i industriella informations- och styrsystem av betydelse för samhällsviktig verksamhet inom kommunalteknisk försörjning.

Kommunen ställer krav på informationssäkerhet i förhållande till andra aktörer

- när informationshantering upphandlas av extern leverantör
- när kommunal verksamhet upphandlas av extern leverantör.

GDPR – Dataskyddsförordningen

I maj 2018 trädde den nya dataskyddsförordningen (GDPR, The General Data Protection Regulation) i kraft. Dataskyddsförordningen gäller i hela EU och efterträder den tidigare Personuppgiftslagen (PUL). [4]

Ett av syftena med dataskyddsförordningen (GDPR) är att skydda medborgarnas grundläggande rättigheter och friheter och då särskilt deras rätt till skydd av personuppgifter.[5]

För Borås Stads och andra kommuners del innebär GDPR att flera aspekter måste beaktas när det gäller hanteringen av medborgares och anställdas personuppgifter. GDPR ställer krav på hur organisationen ska utformas, kontrollen av personuppgiftshantering och att det ska finnas personuppgiftsansvariga som tillser att lagstiftningen efterlevs och dataskyddsombud som finns som stöd och utövar tillsyn. Medborgare har enligt GDPR rätt att veta vilka

[3] Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser, MSBFS 2015:5 https://www.msb.se/siteassets/dokument/regler/rs/15e78831-767b-4714-9fa4-3b4fd0df92a8.pdf

[4] Integritetsskyddsmyndigheten – Dataskyddsförordningen, Syfte och tillämpningsområde https://www.imy.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-syfte-och-tillampningsomrade/

[5] Ibid.

personuppgifter som finns och hur dessa hanteras. De har också rätt till rättelse av felaktiga uppgifter.

Personuppgifter får bara behandlas om de uppfyller de krav som finns i GDPR.[6]

Offentlighetsprincipen innebär att var och en har rätt att hos myndigheter, som exempelvis kommuner, ta del av allmänna handlingar. Dataskyddsförordningen hindrar inte att personuppgifter i allmänna handlingar lämnas ut för att kommuner ska kunna uppfylla skyldigheten att lämna ut allmänna handlingar enligt offentlighetsprincipen. Om kommunen väljer att lämna ut allmänna handlingar digitalt, vilket blir allt vanligare, krävs dock att reglerna i dataskyddsförordningen följs. Känsliga personuppgifter som utlämnas på detta sätt måste t.ex. skyddas genom lämpliga säkerhetsåtgärder.[7]

NIS-direktivet

NIS-direktivet, som precis som GDPR är ett EU-direktiv, infördes i Sverige 2018 och ställer krav på säkerhet i nätverk och informationssystem. Syftet är att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Kraven i direktivet omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster.[8] Direktivet införlivas i den svenska rättsordningen genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174).

Kommuner kan beröras av NIS-regleringen som leverantörer av samhällsviktiga tjänster så som dricksvatten, energi samt hälso- och sjukvård. Huvudman för berörda tjänster är enligt lagstiftningen skyldig att anmäla sig till respektive tillsynsmyndighet. För sektorn hälso- och sjukvård är Inspektionen för vård och omsorg (IVO) ansvarig tillsynsmyndighet.[9]

Granskningsresultat

Stadsrevisionen har genomfört en uppföljande granskning av tidigare granskning av informationssäkerhet samt granskat hur Borås Stad implementerat GDPR. I materialet nedan är bedömningarna från år 2017 i kursiv stil och nedanför dessa redovisas granskningsresultat och bedömningar för 2020.

[6] SKR, PM Allmänna Dataskyddsförordningen https://skr.se/download/18.61e0690f1635e1fcddc2288e/1526455345783/pm-skl-dataskyddsforordningen-GDPR.pdf

[7] Integritetsskyddsmyndigheten – Vägledningar för myndigheter https://www.imy.se/vagledningar/for-myndigheter

[8] Myndigheten för samhällsskydd och beredskap – NIS-direktivet https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

[9] SKR – NIS-direktivet https://skr.se/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/informationssakerhet/nisdirektivet.19091.html

Informationssäkerhet

Central samordning

Stadsrevisionen konstaterade att det saknades någon särskilt utsedd person som arbetade med övergripande informationssäkerhetsfrågor. Stadsrevisionen konstaterade också att det är väsentligt att Kommunstyrelsen i utvecklingsarbetet säkerställer att informationssäkerheten är tillfredsställande i såväl förvaltningar som bolag. Det saknades tillfredsställande avtal med tekniska och rättsliga begränsningar som hindrar systemleverantör att ta del av uppgifter som Borås Stad gör tillgängliga via säkerhetskopiering. Kommunstyrelsen och berörda nämnder bedömdes behöva säkerställa att samtliga avtal som reglerar hanteringen av sekretessbelagda uppgifter var förenliga med offentlighets- och sekretesslagen.

Det primära uppdraget med att samordna informationssäkerheten ligger på Stadsledningskansliet. Sedan maj 2018 har Borås Stad en informationssäkerhetssamordnare som är anställd för att arbeta med det övergripande informationssäkerhetsarbetet i Borås Stad och införa ett nytt ledningssystem för staden enligt standarden ISO 27 000.

Enligt de intervjuade saknade Borås Stad en övergripande insats för att behandla GDPR-frågor vid införandet 2018, vilket påverkat arbetet med informationssäkerhet. Ingen tjänsteperson var anställd med uppgiften att samordna för införandearbetet. Detta ledde till att informationssäkerhetssamordnaren istället arbetat med GDPR och att informationssäkerhetsarbetet de senaste åren har fått stå tillbaka.

Informationssäkerhetssamordnaren ansvarar för IT-samordnarmöten med representanter från stadens förvaltningar. Mötena hålls med viss regelbundenhet. Mötenas fokus har fram tills nu varit mer inriktat på GDPR snarare än informationssäkerhet.

Rutiner och regler i Borås Stad avseende informationssäkerhet

Stadsrevisionen konstaterade att den interna kontrollen avseende informationssäkerhet inte var tillfredsställande. De brister som identifierades bedömdes främst bero på att Borås Stad till stor del saknade uppdaterade policys och rutiner för informationssäkerhet. De dokument som fanns hade i flertalet fall inte beslutats i enlighet med delegationsordningen. Stadsrevisionen noterade också att inga utbildningar inom informationssäkerhet genomfördes.

Borås Stad har ingen av Kommunstyrelsen eller Kommunfullmäktige fastställd informationssäkerhetspolicy. I dagsläget finns lokala dokument om informationssäkerhet på

vissa förvaltningar. Det finns dock inga övergripande styrdokument, vilket Stadsrevisionen också påpekade i rapporten 2017.

Informationssäkerhetssamordnaren har tagit fram ett nytt styrdokument med en gemensam informationssäkerhetspolicy för Borås Stad, baserat på standarden ISO 27 000[10], som planeras att antas i Kommunstyrelsen och Kommunfullmäktige under 2021. Dokumentet beskriver hur stadens övergripande arbete med informationssäkerhet ska fungera. Planen är att Kommunfullmäktige därefter delegerar beslutsrätten om övriga mer detaljerade dokument till Kommunstyrelsen. Varje nämnd får därefter anta mer specifika anvisningar för sin förvaltning. Policyn skickades ut på remiss till samtliga nämnder den 2 november 2020 och remissvaren ska vara inkomna till Stadsledningskansliet senast den 31 december 2020.

Informationssäkerhetssamordnaren har också köpt in och tagit fram två webbutbildningar, DISA informationssäkerhetsutbildning och GDPR – Dataskydd i offentlig miljö, som finns tillgängliga för alla stadens medarbetare via intranätet.

Dataservice

Dataservice är en avdelning under Servicekontoret som är operativt ansvarig för drift av stadens IT-miljö och IT-säkerhet.

Informationssäkerhet sätter ramarna för arbetet med IT-säkerhet och vilken nivå denna ska ligga på, exempelvis vilken typ av skydd som krävs. Dataservice kan inte själva besluta om vilken nivå av informationssäkerhet som är nödvändig utan det beslutet måste tas av ansvarig nämnd som är ansvarig för sin egen data. Enligt de intervjuade saknas styrdokument och politiskt satta mål för informationssäkerhet, vilket därmed också påverkar hur arbetet med IT-säkerhet utformas. Arbetet har hittills istället skett enligt metoder som tjänstepersonerna själva bedömt som adekvata.

Högre skyddsnivåer inom IT-säkerhet leder också till högre kostnader för staden. För att utveckla IT-säkerhet krävs det att man vet vad som är viktigt och vad som ska prioriteras, vilket de intervjuade upplever till viss del har saknats i styrningen.

Sammanfattning

Stadens har sedan 2018 en informationssäkerhetssamordnare. Arbetet med informationssäkerhet har de senaste åren till stor del fått stå till sidan för arbetet med GDPR. Borås Stad har ingen av Kommunstyrelsen eller Kommunfullmäktige fastställd informationssäkerhetspolicy. Avsaknaden av styrdokument och politiskt satta mål för informationssäkerhet har också påverkat utformandet av stadens arbete med IT-säkerhet. Stadsrevisionen noterar att arbetet med antagande av en ny informationssäkerhetspolicy och styrdokument baserat på standarden ISO 27 000 pågår.

GDPR

Central samordning

Den centrala samordningen av GDPR-frågor har skötts av informationssäkerhetssamordnaren sedan 2018. En stor del av informationssäkerhetssamordarens arbete fram tills nu har bestått av GDPR, snarare än informationssäkerhet.

Dataskyddsombud (DSO)

GDPR ställer krav på att varje myndighet ska ha dataskyddsombud. Som en effekt av införandet av GDPR har Borås Stad sedan 2018 två dataskyddsombud som övervakar att organisationen följer dataskyddsförordningen. Dataskyddsombuden är anställda av Sjuhärads kommunalförbund och arbetar mot och är utsedda av respektive nämnd och bolagsstyrelse. Uppdraget är tudelat och består dels av en rådgivande roll, dels av en granskande roll. Dataskyddsombuden styrs inte av beslut på politisk nivå eller tjänstemannanivå utan granskningarna följer Integritetsskyddsmyndighetens (tidigare Datainspektionens) tillsynsplan och fokuserar på särskilt kritiska och svårhanterliga områden där man vill hitta praxis.

DSO och informationssäkerhetssamordnaren har möten varje vecka. Kontakten mellan förvaltningarna och DSO har blivit mer och mer fristående och förvaltningarna har hänvisats att kontakta dem direkt vid frågor istället för att kontakta informationssäkerhetssamordnaren.

Nämndernas och bolagens arbete med GDPR

Gällande personuppgiftsbehandling är varje förvaltning en egen myndighet med eget ansvar för sina uppgifter och behandlingar, det vill säga varje förvaltning är personuppgiftsansvarig (PUA). Respektive förvaltning utser en ansvarig tjänsteman för att arbeta med frågorna, en så kallad dataskyddskontakt. Varje dataskyddskontakt ska årligen rapportera till nämnden om antalet uppgifter som inkommit.

Vissa förvaltningar arbetar i kluster med GDPR-arbetet.

[10] Informationssäkerhet.se Ledningssystem för informationssäkerhet https://www.informationssakerhet.se/stod--vagledning/standarder-for-informationssakerhet/ledningssystem-for-informationssakerhet/

De kommunala bolagen är inte del av den centrala samordningen av GDPR. Det finns dock en framarbetad överenskommelse mellan respektive bolag och dataskyddsombuden som fastställts av respektive bolagsstyrelse.

Intern kontroll

I dagsläget har vissa nämnder med dataskyddsförordningen/GDPR i sin interna kontrollplan (Överförmyndarnämnden, Valnämnden, Servicenämnden, Miljö- och konsumentnämnden och Fritids- och folkhälsonämnden). Individ- och familjeomsorgsnämnden har med informationssäkerhet i sin interna kontrollplan.

Dataskyddsförordningen/GDPR eller informationssäkerhet finns inte med i Kommunstyrelsens plan för intern kontroll.

Borås Stad har riktlinjer för intern kontroll som beslutas av Kommunstyrelsen. I riktlinjerna finns ingen information om att informationssäkerhet ska ingå i nämndernas interna kontroll.

Enligt standarden ISO 27 000 behöver förvaltningens arbete med informationssäkerhet ingå i nämndens arbete med intern kontroll. Detta är också ett av kraven i utkastet till Borås Stads nya informationssäkerhetspolicy.

System för hantering av personuppgifter

Sedan 2018 har staden infört flera system för att hantera personuppgifter.

Selfpoint är en e-tjänst som Borås Stad använder vid begäran om registerutdrag av personuppgifter. Då förfrågningar kommer in till förvaltningen skickas mejl ut till utsedda kontaktpersoner som sedan går in i systemet och hanterar begäran. Förfrågningarna ska hanteras inom 30 dagar och informationssäkerhetssamordnaren har behörighet att se samtliga förfrågningar för att säkerställa att ingen blir liggande. De intervjuade menar att det fanns viss förvirring vid införandet av rutinen som ledde till att förfrågningar blev liggande, men att det nu fungerar relativt väl. Fler personer har nu tillgång till systemet vilket gör att förfrågningar kan upptäckas och hanteras snabbare.

Draftit Privacy Records är ett digitalt verktyg där samtliga personuppgiftsbehandlingar kan registreras. Verktyget används av samtliga förvaltningar för att hantera personuppgifter. I Draftit kan man också se statistik för överföring av personuppgifter till tredje part. Enligt de intervjuade fungerar systemet och hanteringen bra.

KLASSA är ett digitalt verktyg, framtaget av SKR, som används i Borås Stads verksamheter för att säkerhetsklassa information. Verktyget används för att göra en bedömning av vilken säkerhetsnivå olika verksamhetssystem behöver och vilka konsekvenser som uppstår om informationen inte kan nås, om den kan förvanskas eller kommer på avvägar.

Varje förvaltning måste klassificera sin egen data, vilket skyddsbehov som finns och hur den ska hanteras. Dataservice för i vissa fall dialog med dataskyddskontakterna om hur olika system har klassats, vilken skyddsnivå detta kräver och vilken kostnad det blir. En stor del av arbetet med informationssäkerhetsklassning och registervård sker direkt mellan respektive förvaltning och DSO samt informationssäkerhetsansvarig. Prioriteringen görs av förvaltningen med stöd av dataskyddsombuden.

Riktlinjer och dokumentation

Enligt de intervjuade saknade Borås Stad en övergripande insats för att behandla GDPR-frågor vid införandet 2018, vilket ledde till att informationssäkerhetsarbetet de senaste åren till viss del har fått stå till sidan för arbetet med GDPR.

De intervjuade menar att vid införandet saknades dokumentation av befintliga rutiner för hantering av personuppgifter. Det saknades även gemensamma metoder. De intervjuade uppger att Borås Stad arbete med riktlinjer och dokumentation för GDPR var eftersatt i jämförelse med andra kommuner. Arbetet inleddes därför med en omfattande kartläggning av de existerande rutinerna, vilket ledde till att själva arbetet med att införa nya rutiner försenades.

De intervjuade menar att det tagit tid att förankra system, rutiner och processer för arbetet med GDPR i staden, men upplever att dessa nu i många delar är på plats. Detta gör att man framöver kan fokusera mer på det centrala informationssäkerhetsarbetet där även GDPR ingår.

Införandet av Office 365

Den 16 juli 2020 slog EU-domstolen fast att det så kallade Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Ogiltigförklarandet innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att med *Privacy Shield* som grund överföra personuppgifter till mottagare i USA.[11]

[11] Integritetsskyddsmyndigheten – Så här påverkar Schrems II-domen överföringar till tredje land https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/sa-har-paverkar-schrems-ii-domen-overforingar-till-tredje-land/

Domen påverkar alla organisationer som använder amerikanska IT-tjänster, exempelvis den molnbaserade tjänsten Office 365 som Borås Stad har planerat att införa och som är en del av stadens ökade digitalisering. Informationsöverföringen till tredje part, i vissa fall av sekretessbelagda uppgifter och personuppgifter, ställer krav på att informationssäkerheten beaktas i utformandet av avtal.

Borås Stads IT-råd lämnade den 24 augusti 2020 en rekommendation till Kommunstyrelsen om att besluta att planering av införandet av Office 365 kan inledas, samtidigt som det oklara rättsläget kräver en kontinuerlig bevakning av rättsläget på området för att eventuellt omvärdera tidigare ställningstaganden. I skrivelsen Sammanvägd bedömning av Office 365 framhöll IT-rådet också att införandet kräver vissa försiktighetsåtgärder, inte minst för att göra det tydligt för den enskilde medarbetaren hur och var olika uppgifter ska hanteras och underlätta för denne att göra rätt.

Skrivelsen drogs tillbaka då vissa juridiska frågetecken kvarstår. Den håller på att ses över och en ny kompletterande version kommer enligt uppgift från intervjuade att tas upp till Kommunstyrelsen för beslut under första kvartalet 2021. Dataskyddsombuden har under hösten till flera förvaltningar starkt rekommenderat att alla projekt och införanden av tredjelandsbaserade molntjänster ska bromsas upp och pausas.

Sammanfattning

Stadens centrala samordning av GDPR har skötts av informationssäkerhetssamordnaren sedan 2018. Staden har sedan 2018 två dataskyddsombud som stöttar nämndernas arbete med GDPR. Sedan dess har nya system och utbildningar för hantering av personuppgifter införts. Vid införandet av GDPR saknades tydliga riktlinjer och dokumentation för att behandla GDPR-frågor, vilket lett till att arbetet med att införa rutiner försenats. Arbetet med införandet av Office 365 påverkas också av GDPR och har för närvarande pausats då vissa juridiska frågetecken kvarstår.

NIS-direktivet

För Borås Stad berör NIS-direktivet Vård- och äldrenämnden (inom hälso- och sjukvård) och de kommunala bolagen (Borås Elnät, Borås Energi och Miljö AB). De kommunala bolagen ingår inte i samordningsarbetet på samma sätt gällande NIS och GDPR men kommer att inkluderas i informationssäkerhetspolicyn som berör hela staden.

Då NIS-direktivet enbart berör Vård- och äldrenämnden är det inte en stadenövergripande fråga på samma sätt.

Enligt NIS-direktivet behöver Vård- och äldrenämnden anmäla sin verksamhet till IVO. [12] Enligt de intervjuade hade nämnden missat att anmäla sin verksamhet och blev därför belagda med vite. Nämnden har nu anmält sin verksamhet.

Sammanfattning och iakttagelser avseende Borås stads informationssäkerhetsarbete samt införande av GDPR och NIS-direktivet

De intervjuade menar att rutiner och processer för arbetet med GDPR i staden i många delar är på plats, vilket gör att man nu kan fokusera mer på det centrala informationssäkerhetsarbetet. Detta arbete berör också det fortsatta arbetet med GDPR då många processer och policyer inbegriper både arbetet med GDPR och informationssäkerhet.

De intervjuade framhåller att framtida utmaningar inom informationssäkerhetsarbetet i staden grundar sig i lärdomar från GDPR-införandet, vilka bland annat är vikten av samordning, resurser och tid. Utan ett gemensamt styrdokument har det varit svårt att få samtliga förvaltningar att enas. Den mängd resurser och tid som ges för att arbeta med informationssäkerhet är också avgörande, likaså påverkar kontaktpersonernas/dataskyddskontakternas status på förvaltningen. Till viss del är arbetet personberoende och en avgörande framgångsfaktor har varit att ha engagerade tjänstepersoner som är insatta i frågan i de fall där styrdokument och tydliga instruktioner saknats. En ytterligare framtida utmaning är kommunikation, då ett gediget informationsarbete krävs för att nå ut med informationen på förvaltningarna.

Stadsrevisionens bedömning

Stadsrevisionen har genomfört en uppföljande granskning utifrån granskningen av Borås Stads arbete med informationssäkerhet som genomfördes år 2017. Uppföljningens övergripande syfte är dels att genomföra en uppföljning av tidigare granskning av informationssäkerhet, dels att granska hur Borås Stad implementerat GDPR och NIS-direktivet.

[12] IVO – Anmälan för leverantörer av samhällsviktiga tjänster https://www.ivo.se/for-yrkesverksamma/informationssakerhet/anmalan-for-leverantorer-av-samhallsviktiga-tjanster/

De huvudsakliga revisionsfrågorna är att undersöka vilka styrdokument och planer som Borås Stad har inom området, hur arbetet för att säkerställa förutsättningar för god informationssäkerhet utvecklats sen 2017, om Kommunstyrelsen säkerställer en tillräcklig intern kontroll avseende den övergripande informationssäkerheten samt hur Kommunstyrelsen har bedrivit arbetet med att implementera GDPR och NIS-direktivet.

Granskningen visar att arbetet med informationssäkerhet i stora delar nedprioriterats sedan 2017 på grund av otillräcklig planering och prioritering avseende det centrala införandebetet med GDPR. Detta har inneburit att resurser som avsatts för arbete med informationssäkerhet istället avletts till arbete med införandet av GDPR. Informationssäkerhetssamordnaren har istället för att arbeta med informationssäkerhet fått fokusera på framtagandet av rutiner samt centrala samordningen för GDPR-arbetet. Arbetet med framtagande av tydliga strukturer för informationssäkerhet har under 2020 kunnat prioriteras i stötte utsträckning och framtagande av en ny informationssäkerhetspolicy pågår och beräknas slutföras under 2021.

Granskningen visar att det inte finns några övergripande planer eller styrdokument gällande informationssäkerhet. Området saknar även en tydligt formulerad målsättning. Stadsrevisionen kan konstatera att de brister som identifierades i 2017 års granskning i dessa delar till största delen kvarstår. Förhållandena medför enligt stadsrevisionens bedömning att styrningen av hur Borås Stads informationssäkerhetsarbete ska bedrivas varit bristfällig under en längre tid.

Förhållandena har inneburit att arbetet hittills skett utan tydliga riktlinjer, vilket riskerat att leda till att informationssäkerhetsfrågor och GDPR-frågor hanterats olika i förvaltningarna. Bristen på styrning har inneburit risk för att tjänstepersoner i Stadens förvaltningar fått fatta strategiska beslut utan övergripande vägledning och politisk förankring.

Borås Stad har sedan 2017 en informationssäkerhetssamordnare, utsedda dataskyddsombud och det finns en dataskyddskontakt vid varje förvaltning. Webbutbildningar inom informationssäkerhet och GDPR har införts, likaså nya system för hantering av GDPR-frågor. Stadsrevisionen bedömer att arbetet för att säkerställa förutsättningar för god informationssäkerhet i dessa delar har utvecklats positivt sedan 2017.

Granskningen visar vidare att vissa nämnder på egen hand har inkluderat GDPR/informationssäkerhet i arbetet med interna kontroll. Det är dock inte inkluderat i Kommunstyrelsens riskanalys eller plan för intern kontroll. Det saknas därutöver anvisningar som avser informationssäkerhetsaspekter i Borås Stads regler för intern kontroll eller vägledningsdokumentet intern kontroll i Borås Stad.

Stadsrevisionens bedömning är att Kommunstyrelsen bör förtydliga regler och vägledning för intern kontroll för att säkerställa att risker inom informationssäkerhetsområdet inkluderas i nämndernas arbete med intern kontroll. Inte minst är detta betydelsefullt för att säkerställa följsamhet till standarden ISO 27 000. Stadsrevisionen noterar att detta ingår som en del i förslaget på ny informationssäkerhetspolicy.

NIS-direktivet berör enbart Vård- och äldrenämnden samt vissa av de kommunala bolagen. Vård- och äldrenämnden hade missat att anmäla sin verksamhet till Inspektionen för vård och omsorg (IVO) och blev därför belagda med vite. Nämnden har nu anmält sin verksamhet i enlighet med NIS-direktivet.

Sammanfattande bedömning

Sammanfattningsvis visar granskningen att arbetet med informationssäkerhet i stora delar nedprioriterats sedan 2017 på grund av otillräcklig planering och prioritering avseende det centrala införandebetet med GDPR. Förutsättningarna för arbetet med informationssäkerhet/GDPR har i vissa delar utvecklats positivt sedan 2017. Dock är flera av de brister som konstaterades i granskningen 2017 fortsatt aktuella. Bland annat saknas central styrning och styrande dokument på övergripande nivå gällande informationssäkerhet. Vidare är det inte säkerställt att olika aspekter av informationssäkerhet/GDPR är inkluderat i nämndernas arbete med intern kontroll.

Stadsrevisionen noterar att arbete med en ny informationssäkerhetspolicy för Borås Stad pågår. Stadsrevisionen ser positivt på det påbörjade arbetet i dessa delar.

Stadsrevisionen bedömer sammanfattningsvis att den interna styrningen och kontrollen av arbetet med informationssäkerhet i Borås Stad inte är helt tillräcklig

Källförteckning

Lagar och förordningar
Kommunallagen
Tryckfrihetsförordningen
Offentlighets- och sekretesslagen
Arkivförordningen
Arkivlagen
Dataskyddsförordningen
NIS-direktivet

Internetkällor
Borås Stad – Informationshantering och arkiv
https://intranet.boras.se/styrningochledning/handbockermetodermodellerochruti-ner/offentligforvaltning/informationshanteringocharkiv.4.613655ff148a1209d2d49f31.html

Informationssäkerhet.se Ledningssystem för informationssäkerhet
https://www.informationssakerhet.se/stod--vagledning/standarder-for-informationssakerhet/ledningssystem-for-informationssakerhet/

Integritetsskyddsmyndigheten – Dataskyddsförordningen, Syfte och tillämpningsområde
https://www.imy.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-syfte-och-tillampnings-omrade/

Integritetsskyddsmyndigheten – Så här påverkar Schrems II-domen överföringar till tredje land
https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/sa-har-paverkar-schrems-ii-domen-overforingar-till-tredje-land/

Integritetsskyddsmyndigheten – Vägledningar för myndigheter
https://www.imy.se/vagledningar/for-myndigheter/

IVO – Anmälan för leverantörer av samhällsviktiga tjänster
https://www.ivo.se/for-yrkesverksamma/informationssakerhet/anmalan-for-leverantorer-av-samhallsviktiga-tjanster/

Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser, MSBFS 2015:5
https://www.msb.se/siteassets/dokument/regler/rs/15e78831-767b-4714-9fa4-3b4fd0df92a8.pdf

Myndigheten för samhälsskydd och beredskap – NIS-direktivet
https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

SKR – NIS-direktivet
https://skr.se/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/informationssakerhet/nisdirektivet.19091.html

SKR, PM Allmänna Dataskyddsförordningen https://skr.se/download/18.61e0690f1635e1fcdd-c2288e/1526455345783/pm-skl-dataskyddsforordningen-GDPR.pdf

BORÅS STAD

STADSREVISIONEN

Besöksadress Sturegatan 42 **Postadress** 501 80 Borås
Telefon 033-35 71 56 **E-post** revisionskontoret@boras.se
Webbplats boras.se/stadsrevisionen