Uppföljande granskning av efterlevnad av GDPR

Rapport

Luleå kommun

KPMG AB

2022-03-11

Antal sidor 12

Luleå kommun
Uppföljande granskning av efterlevnad av GDPR

2022-03-11

Innehållsförteckning

1 Sammanfattning

Vi har av Luleå kommuns revisorer fått i uppdrag att genomföra en uppföljande granskning av 2019 års granskning gällande kommunens efterlevnad av GDPR. Uppdraget ingår i revisionsplanen för år 2021.

Syftet med granskningen är att följa upp hur arbetet med rutiner för efterlevnad av dataskyddsförordningen har fortlöpt.

Vår sammanfattande bedömning utifrån granskningens syfte är att det till viss del finns rutiner och en organisation för att säkerställa sitt arbete med GDPR. Vi bedömer att det fortsatt finns behov av att säkerställa de registrerades rättigheter samt att utbildningsnivån inom hela koncernen behöver stärkas. Vi anser således att det fortsatt finns ett arbete med att säkerställa en fullständig efterlevnad av GDPR-lagstiftningen.

Mot bakgrund av vår granskning rekommenderar vi att:

- kommunstyrelsen tillser att förvaltningarna säkerställer att det i varje personuppgiftsbehandling finns dokumenterade rutiner för de registrerades rättigheter gällande information, registerutdrag, radering, rättning, invändning, begränsning och dataportabilitet, se avsnitt 3.3
- kommunstyrelsen säkerställer att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare, se avsnitt 3.3

2 Inledning/bakgrund

2019 genomförde Luleå kommuns revisorer en granskning av kommunens rutiner för efterlevnad av dataskyddsförordningen (hädanefter GDPR). De förtroendevalda revisorerna utgick utifrån risk- och väsentlighet valde att granska kommunens övergripande arbete med att GDPR. Det bedömdes föreligga risk för att verksamheterna inte färdigställt allt som behöver anpassas samt införas och bedömde det därför som väsentligt att detta område skulle granskas.

Den sammanfattande bedömning utifrån granskningens syfte var att kommunen till stor del har rutiner och en organisation för att säkerställa sitt arbete med GDPR. Ansvar för GDPR och roller behövde i vissa delar förtydligas och förbättringsarbetet genomföras med en större systematik. Vid tiden för granskningen genomfördes arbetet till stor del reaktivt på grund av händelser som kräver åtgärd och inte proaktivt för att exempelvis registerförteckningar ska vara kompletta eller förhindra att incidenter sker. Det genomfördes en regelbunden uppföljning över hur väl kommunen uppfyller de lagkrav som finns vilket resulterar i att medvetande om brister och behov av åtgärder är hög. Att säkerställa kommunens efterlevnad av GDPR är ett pågående arbete och en stor del av arbetet kvarstod vid tiden för granskningen för att efterleva lagen fullt ut.

Då det nu har gått en tid avser revisionen att följa upp området.

2.1 Syfte, revisionsfråga och avgränsning

Den uppföljande granskningen syftar till att följa upp hur arbetet med rutiner för efterlevnad av dataskyddsförordningen har fortlöpt.

Granskningen omfattar kommunens övergripande rutiner för efterlevnad av GDPR.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
- Internt styrande dokument.

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av relevanta dokument såsom nulägesrapport GDPR, Protokollsbeslut, internkontrollplan räddningstjänsten, internkontrollplan
- Avstämningar med berörda tjänstepersoner däribland: Dataskyddsombud och kommunjurist.

3 Resultat av granskningen

3.1 Granskningen 2019

Vid granskningen som genomfördes under 2019 konstaterades att det till stor del fanns rutiner och en organisation för att säkerställa arbetet med GDPR. Däremot behövde vissa delar kring ansvar och roller förtydligas samt att förbättringsarbetet behövde genomföras med en större systematik.

Det konstaterades samtidigt att det proaktiva arbetet behövde stärkas för att exempelvis registerförteckningarna skulle vara komplette eller förhindra att incidenter sker. Vid tidpunkten för granskningen genomfördes regelbundna uppföljningar som resulterat i högt medvetande om brister och behov. Det konstaterades att säkerställandet av GPDR efterlevnad i kommunen var ett pågående arbete och en stor del av det arbetet kvarstod för att kunna efterleva lagen fullt ut.

Mot bakgrund av granskningen 2019 rekommenderade vi kommunstyrelsen att:

- säkerställa att dataskyddsombud involveras och rådfrågas i högre grad i alla frågor som rör skyddet av personuppgifter
- tydliggöra roll och förväntningar på utsedda personuppgiftsombud i förvaltningarna och säkerställa att dessa inte har någon intressekonflikt med övriga uppdrag
- säkerställa att GDPR-arbetet sker på ett likvärdigt sätt i alla förvaltningar
- använda de resultat som framkommit i intern revision och nulägesanalys för att prioritera åtgärder och genomföra dessa på ett systematiskt sätt med tillräckliga resurser
- tillse att förvaltningarna säkerställer att det i varje personuppgiftsbehandling finns dokumenterade rutiner för de registrerades rättigheter gällande information, registerutdrag, radering, rättning, invändning, begränsning och dataportabilitet
- utifrån kontrollmål för efterlevnad av GDPR i internkontrollplan för 2020 bedöma risk och konsekvenser för brister i efterlevnad av GDPR och kontrollåtgärder för dessa
- säkerställa att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare då dessa är obligatoriska och nödvändiga för att medvetenheten om hantering av personuppgifter ska vara tillräcklig

3.2 Organisation och ansvarsfördelning

Nedan redovisas de svar som lämnades vid 2019 års granskning samt en nulägesbild.

3.2.1 Dataskyddsombud

Att kommunstyrelsen säkerställer att dataskyddsombudets involveras och rådfrågas i högre grad i alla frågor som rör skyddet av personuppgifter

Kommunstyrelsens yttrande

Kommunstyrelsen meddelade i sitt svar att kommunstyrelsens målsättning är att förvaltningarna själv ska omhänderta frågor i så stor utsträckning som möjligt men att dataskyddsombudet givetvis ska involveras och rådfrågas vid behov. Dataskyddsombudet rådfrågas alltid vid komplicerade personuppgiftsincidenter och vid situationer där rättsläget är osäkert.

I rapporten hänvisas till dataskyddsstyrelsens råd där det framgår att dataskyddsombudet ska inbjudas att delta i möten på högsta och mellanliggande förvaltningsnivå och att dataskyddsombudets åsikt alltid måste ges tillbörlig vikt. Kommunstyrelsen har för avsikt att se över rutiner för dataskyddsombudets involvering i ledningsfrågor.

Nuläge 2021

Vi har inte erhållit fullständiga uppgifter, komplettering sker under våren 2022

3.2.2 Likvärdigt arbete

Att kommunstyrelsen säkerställer att GDPR-arbetet sker på ett likvärdigt sätt i alla förvaltningar

Kommunstyrelsens yttrande

Kommunstyrelsen meddelade i sitt svar att I detta sammanhang är det viktigt att betona att alla kommunala nämnder och bolag är personuppgiftsansvariga vilket innebär att varje nämnd/styrelse ansvarar för att GDPR-arbetet inom dess verksamhet sker i enlighet med gällande lagstiftning. Kommunstaben har enbart en stödjande roll gentemot övriga förvaltningar och kan därmed inte ställa krav på förvaltningarna. Däremot kan kommunstaben se till att det finns förutsättningar för ett likvärdigt arbete inom kommunen.

Sedan inträdet av GDPR har kommunstaben haft en inofficiell roll som samordnande förvaltning utifrån det arbete som dataskyddsombudet och GDPR-strategen utfört. Det samordnande arbetet har skett genom utbildningar och regelbundna möten med personuppgiftsombud från andra förvaltningar och kommunala bolag.

För närvarande genomförs en hel del arbete för att skapa enhetlighet inomkommunen. Som exempel är GDPR-strategen för närvarande involverad i PM³-projektet med syfte att säkerställa att GDPR-arbetet blir en naturlig del i systemförvaltningsarbetet. I det arbetet ingår bl.a. att skapa gemensamma mallar för GDPR-arbetet.

Till årsskiftet planeras även att lansera möjligheten att bli en GDPR-diplomerad arbetsplats för att kunna visa att verksamheten tar GDPR-frågorna på allvar. Diplomeringen riktar sig till samtliga förvaltningar och kommunala bolag.

Nuläge 2021

Vi har inte erhållit fullständiga uppgifter, komplettering sker under våren 2022

3.2.3 Tydliggörande av roller

Att kommunstyrelsen tydliggör roller och förväntningar på utsedda personuppgiftsombud och säkerställer att dessa inte har någon intressekonflikt med övriga uppdrag.

Kommunstyrelsen yttrande

Kommunstyrelsen lämnade som svar att den 21 februari 2020 beslutades det om en ny dataskyddsorganisation med fokus på hanteringen av GDPR-arbetet inom förvaltningarna. Syftet med dataskyddsorganisationen är att tydliggöra de olika rollerna och deras funktioner. I detta ingår även att tydliggöra rollerna för de utsedda personuppgiftsombuden.

Kommunstyrelsen har säkerställt att utsedda personuppgiftsombud i de förvaltningar som kommunstyrelsen ansvarar för inte har någon intressekonflikt med övriga uppdrag.

Nuläge 2021

Vi har inte erhållit fullständiga uppgifter, komplettering sker under våren 2022

3.2.4 Internkontroll

Att utifrån kontrollmål för efterlevnad av GDPR i internkontrollplan för 2020 bedöm risk och konsekvenser för brister i efterlevnad av GPDR och kontrollåtgärder för dessa.

Kommunstyrelsens yttrande

Av svaret framkom att det har påbörjats ett arbete med att omhänderta verksamhetens integritetsrisker i processen för intern kontroll. Riskbedömning, planering av åtgärder och kontroller samt uppföljning kommer därmed att integreras i kommunstyrelsens interna kontrollplan

Nuläge 2021

Vi har inte heller erhållit någon internkontrollplan för kommunstyrelsen. Vi kan däremot se att det i bl.a. stadsbyggnadsnämndens internkontrollplan finns en kontrollpunkt som rör GDPR. Vi kan även se att det enligt beslutet för internkontrollplan för 2021 för kommunstaben[1] finns med en kontroll gällande kontrollering och säkerställande att enskilda får information enligt personuppgiftslagstiftning vid identifierade personuppgiftsbehandlingar.

[1] Kommunstyrelsen 2021-03-15, § 60

3.2.5 Bedömning

Vår bedömning är att det finns kontrollmoment i internkontrollplanen för att säkerställa efterlevnaden av dataskydd och GDPR.

3.3 Kommunens arbete för att säkerställa efterlevnad av GDPR

Nedan redovisas de svar som lämnades vid 2019 års granskning samt en nulägesbild.

3.3.1 Personuppgiftsbehandling

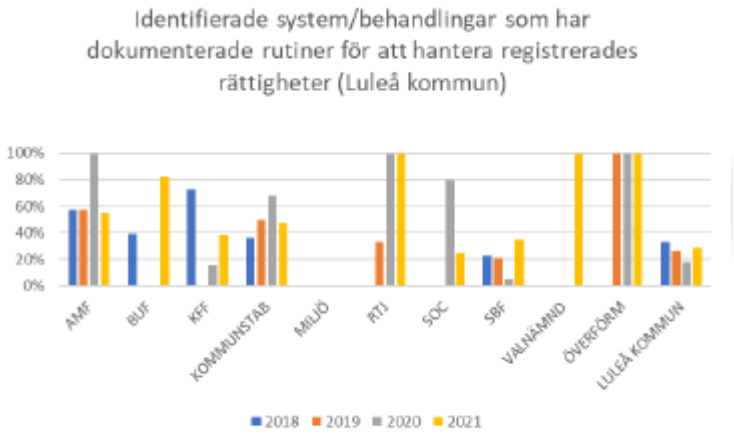
Att kommunstyrelsen tillser att förvaltningarna säkerställer att det i varje personuppgiftsbehandling finns dokumenterade rutiner för de registrerades rättigheter gällande information, registerutdrag, radering, rättning, invändning, begränsning och dataportabilitet

Kommunstyrelsens yttrande

Av svaret framkom att det utifrån de rekommendationer som framkommit av dataskyddsombudets tidigare granskning har kommunstyrelsen påbörjat ett arbete med att upprätta rutiner för att säkerställa de registrerades rättigheter. Kommunstaben arbetar med att utforma rutiner för begäran om registerutdrag. Därefter kommer kommunstaben fokusera på att ta fram ytterligare ruiner för att på ett effektivt sätt kunna hantera de registrerades rättigheter. I dialog med dataskyddsombudet kommer även rutiner för att involvera dataskyddsombudet i ett tidigt skede att utvecklas. Vid tidpunkten då svaret lämnades identifierades även ett behov av att involvera dataskyddsombudet inför inköp av nya IT-system.

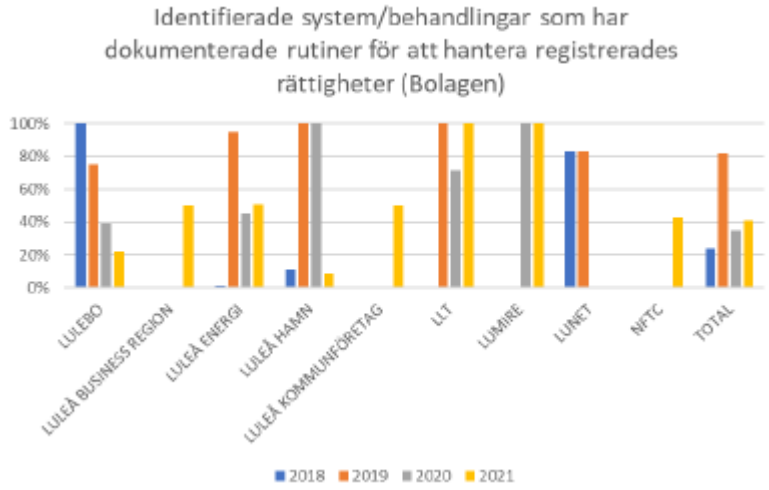
Nuläge 2021

Vi har tagit del av en nulägesrapport gällande nämnders och bolags efterlevnad av GDPR. Enligt rapporten framgår det att de av de identifierade systemen hos Luleå kommun är 29 % (2021) som har dokumenterade rutiner för att hantera de registrerades rättigheter vilket motsvarar en ökning med 11 procentenheter sedan mätningen 2020.



Figur 4: Källa: Luleå kommun

Inom de kommunala bolagen anses 41 % ha dokumenterade rutiner för att hantera de registrerades rättigheter vilket motsvarar en ökning på sex procentenheter sedan 2020. De minskningar som skett hos enskilda bolag är uppmärksammade brister i aktuella rutiner.



Det framgår av uppföljningen att dokumenterade rutiner saknas inte per automatik behöver innebära att registrerades rättigheter inte kan tillgodoses utan påvisar bristande dokumentation

Inom de system som identifieras hos kommunstaben anses 63 % ha dokumenterade rutiner för att hantera de registrerades rättigheter. Då två avdelningar inte redovisade uppgifter vid föregående mätning samt att dessa påvisade avsaknad av rutiner är det en minskning med fem procentenheter sedan mätningen 2020

3.3.2 Utbildning

Att kommunstyrelsen säkerställer att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare då dessa är obligatoriska och nödvändiga för att medvetenheten om hantering av personuppgifter ska vara tillräcklig

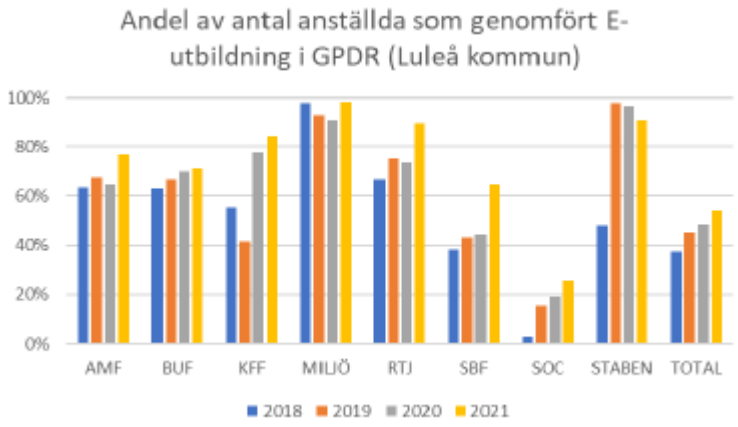
Kommunstyrelsens yttrande

Kommunstyrelsen lämnade som svar att det sedan GDPR trädde i kraft varit ett fokus på att öka medvetenheten om lagstiftningen, som ett led i detta har kommunstyrelsen köpt in en webbaserad utbildning gällande GDPR som är obligatorisk för samtliga medarbetare. Uppföljningen av detta sker löpande och vid senaste uppföljningen (september 2021) kunde det konstateras att 99 % av kommunstabens medarbetare genomfört utbildningen, 75 % (räddningstjänsten) och 73 % (arbetsmarknadsförvaltningen). Kommunstabens uppfattning är att de flesta medarbetare på förvaltningarna har grundläggande kunskaper inom GDPR-området.

Utöver dataskyddsutbildningen så har även kommunen ytterligare två obligatoriska utbildningar dels datorstödd informationssäkerhetsutbildning för användare (DISA) som tagits fram av myndigheten för samhällsskydd och beredskap samt utbildningen ”Luleå kommun mot korruption” som till viss del innehåller informationssäkerhet. Det åligger närmaste chef att säkerställa att samtliga medarbetare genomfört dessa utbildningar.

Nuläge 2021

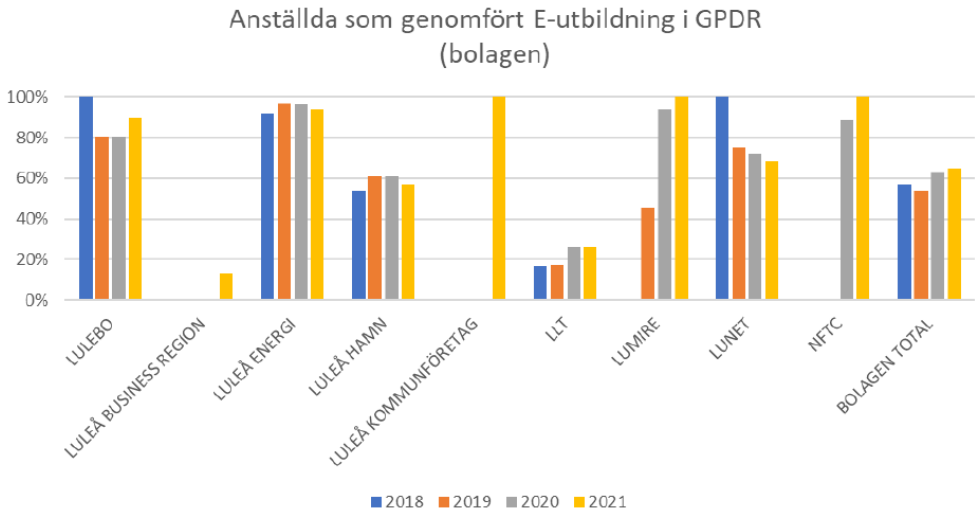
Enligt en nulägesrapport som vi tagit del av gällande GDPR-arbetet framgår att E-nämnden har upphandlat en E-utbildning för att ge kommunkoncernen en möjlighet att säkerställa en grundnivå på kunskapen inom GDPR. Det framgår att vissa organisationer har valt andra metoder för att säkerställa en grundnivå på kunskap detta bl.a. då viss personal inte har tillgång till dator i arbetet vilket förekommer i högre utsträckning inom socialnämnden, Lumire och Luleå Lokaltrafik AB. Det har tagits fram APT material kring GDPR som kan användas på arbetsplatser där medarbetarna inte har tillgång till dator. Det finns däremot ingen statistik som visar på hur många som fått utbildning i GDPR via APT.



Figur 1: Källa Luleå kommun.

Inom Luleå kommun har 54 % av samtliga anställda genomgått E-utbildning inom GDPR. Detta är en ökning sedan föregående mätning (2020) med fem procentenheter. Arbetsmarknadsförvaltningen 77 %, barn- och utbildningsförvaltningen 72 %, kultur- och fritidsförvaltningen 84 %, räddningstjänsten 90%, stadsbyggnadsförvaltningen 65 %, miljöavdelningen inom stadsbyggnadsförvaltningen 98 %, socialförvaltningen 26 % samt kommunstaben 91 %. Enligt nulägesrapporten framgår att personal inom socialförvaltningen som inte har tillgång till egen dator tagit del av utbildning med hjälp av APT-materialet. Enligt socialförvaltningen har samtliga anställda tagit del av grundutbildningen.

Inom de kommunala bolagen ser vi att resultaten skiljer sig åt. Inom bolagen har totalt 65 % av alla anställda genomfört utbildningen vilket är en förbättring med två procentenheter sedan mätningen 2020.



Figur 2: Källa: Luleå kommun

Inom Luleå kommunföretag, Lumire samt NFTC har samtliga anställda genomfört utbildningen. Lulebo 90 %, Lueå Business Region 13 %, Luleå Energi 94 %, Luleå hamn 57 %, LLT 26 % och Lunet 68 %.

3.3.3 Bedömning

Vår bedömning är att det fortsatt finns brister gällande rutiner för de registrerades rättigheter. Totalt har 29 % av identifierade system/behandlingar dokumenterade rutiner för att hantera registrerades rättigheter. Vår rekommendation från 2019 års granskning kvarstår därmed.

Vi noterar att det är drygt hälften av kommunens medarbetare som genomgått E-utbildningen inom GDPR. Detta resultat dras dock ned av att samtliga inom socialförvaltningen inte genomfört E-utbildningen däremot har detta ersatts med att utbildning genomförts enligt framtaget APT-material. Frånsett socialförvaltningen, som uppger att samtlig personal tagit del av GDPR-utbildningen, har drygt 82 % av övriga

medarbetare tagit del av E-utbildningen kring GDPR. Vi kan dock se en stor variation bland de kommunala bolagen där totalt 65 % genomfört utbildningen.

Vi rekommenderar därför i enlighet med 2019 års granskning att kommunstyrelsen säkerställer att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att det till viss del finns rutiner och en organisation för att säkerställa sitt arbete med GDPR. Vi bedömer att det fortsatt finns behov av att säkerställa de registrerades rättigheter samt att utbildningsnivån inom hela koncernen behöver stärkas. Vi anser således att det fortsatt finns ett arbete med att säkerställa en fullständig efterlevnad av GDPR-lagstiftningen.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen/nämnden att:

- kommunstyrelsen tillser att förvaltningarna säkerställer att det i varje personuppgiftsbehandling finns dokumenterade rutiner för de registrerades rättigheter gällande information, registerutdrag, radering, rättning, invändning, begränsning och dataportabilitet, se avsnitt 3.3
- kommunstyrelsen säkerställer att utbildning i informationssäkerhet och dataskydd genomförs av samtliga medarbetare, se avsnitt 3.3

Datum som ovan

KPMG AB

DocuSigned by:
29FEC0EAB81B46E...

Oskar Nordmark
Certifierad kommunal revisor

DocuSigned by:
E1E5533098AA495...

Eva Henriksson
Certifierad Kommunal revisor