

§ 25

Diarienumr: KS-2020/00867

Svar på revisionsrapport: Granskning av efterlevnad av Dataskyddsförordningen GDPR**Beslut**

Kommunstyrelsen beslutar

att avge svar på revisionsrapport: *Granskning av efterlevnad av Dataskyddsförordningen GDPR* enligt nedan yttrande

att ge förvaltningen i uppdrag att se över de befintliga och kammungemensamma riktlinjerna och rutinerna och vid behov komplettera dessa för såväl GDPR-arbetet och informations-säkerhetsarbetet så att arbetet bedrivs på ett ändamålsenligt sätt.

Ärendebeskrivning

Kommunrevisorerna har granskat efterlevnad av Dataskyddsförordningen GDPR. Kommunstyrelsen har fått förlängd svarstid från 5 februari till 10 februari.

Yttrande

Baserat på den analys och granskning som genomförts bedöms Umeå kommun ha den genomsnittliga mognadsgraden 2,4 av 5,0. 2,4 är en förhållandevis låg nivå jämfört med vad EY generellt observerar för kommuner.

Kommunstyrelsen konstaterar att det sedan dataskyddsförordningens införande har arbetats i förvaltningen för att säkerställa att kommunen uppnår de krav som lagen och invånare ställer men att det återstår mycket arbete då kommunstyrelsen förfogar över en stor mängd personuppgifter vanligtvis hanterade i något av de cirka 40 IT-system som åligger kommunstyrelsens ansvar. Kommunstyrelsen bör sträva efter att som lägst uppnå den genomsnittliga mognadsgraden för kommuner.

Umeå kommuns arbete med personuppgiftshantering har flera förbättringsområden. Det saknas beslutade riktlinjer och rutiner inom ett flertal områden och det återstår mycket operativt arbete för att uppnå en ändamålsenlig nivå. EY rekommenderar att styrningen utvecklas framför allt inom:

- Organisation och ansvar, där resursfördelning och arbetsinstruktioner bör styra arbetet med utformning och dokumentation av övergripande riktlinjer och rutiner mot att samordnas centralt i högre utsträckning, resurser bör tilldelas för operativt arbete i förvaltningarna och informationssäkerhetssamordnarens placering i organisationen bör ses över;

Rekommendationen är rimlig och kommunstyrelsens verksamheter behöver se över resursfördelning utifrån målsättning och arbetets omfattning för en ändamålsenlig informationshantering samt att överväga informationssäkerhetssamordnarens organisatoriska tillhörighet i dialog med berörd teknisk nämnd och teknisk förvaltning (IT-avdelning).

- Kontroll, där man följer upp arbetet regelbundet för att säkerställa att verksamheten lever upp till de krav som lagen, kommunen och dess invånare förväntar sig;

Genom att arbeta efter ett ledningssystemets intention och därigenom strukturera det operativa arbetet möjliggörs att kontrollera och säkerställa att de krav som finns efterlevs.

- Utbildning, där man bör säkerställa att alla medarbetare tar del av regelbundna utbildningar.

Kommunen har genomfört två nanoutbildningar utskickade via e-post. Svarsfrekvensen har inte varit tillfredsställande, endast cirka 30 %. Dataskyddsombudet och informationssäkerhetssamordnaren arrangerar årligen utbildning i samband med dataskyddsdagen men även kontinuerliga utbildningserbudanden till nämnderna och förvaltningarna och till det nätverk som finns med personuppgiftskoordinatorer. Personuppgiftskoordinatorer stöttar i sin tur medarbetare i direkta personuppgiftsfrågor. Många verksamheter har också GDPR som stående punkt på arbetsplatsträffar. Kommunstyrelsen konstaterar att utbildningsbehovet ändå inte är tillgodosett till fullo och att arbete enligt

ett ledningssystemens intention kan bidra till att säkerställa medarbetarnas utbildningsnivå.

Dessa punkter skulle kunna åtgärdas med hjälp av att kommunen implementerar ett ledningssystem för informationssäkerhet (LIS)

Kommunstyrelsen bör på sikt implementera ett ledningssystem för informationssäkerhet men kan redan i nuläget arbeta enligt ett sådant ledningssystemens intention.

Beslutsunderlag

Revisionsrapport.

Beredningsansvariga

Tomas Jakobsson, kommunledningsstaben

Näringslivs- och arbetsutskottets beslutsordning

Yrkanden

Janet Ågren (S) – Bifall till tjänsteskrivelsens förslag med följande tillägg: att ge förvaltningen i uppdrag att se över de befintliga och kommungemensamma riktlinjerna och rutinerna och vid behov komplettera dessa för såväl GDPR-arbetet och informationssäkerhetsarbetet så att arbetet bedrivs på ett ändamålsenligt sätt.

Propositionsordning som godkänns

Bifall mot avslag till tjänsteskrivelsen inklusive Janet Ågrens tillägg.

Ordföranden konstaterar att näringslivs- och arbetsutskottet bifaller tjänsteskrivelsen inklusive Janet Ågrens tillägg.

Beslutet ska skickas till

Kommunrevisorerna (kommunrevisionen@umea.se)

Kommunstyrelsens verksamheter