Västerås stads revisorer

SENASTE NYTT Nr 86 – 2020

Granskning av efterlevnad av GDPR i staden

Granskningens inriktning

På uppdrag av de förtroendevalda revisorerna har EY genomfört en granskning av stadens hantering av personuppgifter och efterlevnad av dataskyddsförordningen GDPR. Syftet har varit att ge en övergripande förståelse av huruvida kommunen bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur väl man uppfyller de åtgärder som förordningen stipulerar.

Iakttagelser och slutsatser

Den samlade bilden är att kommunen initialt valt att prioritera införande av fungerande processer genom verksamheten, vilket EY bedömer har fungerat väl, men att det nu är hög tid att införa strukturerade granskningar och rapportering i relation till arbetet.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under juni till september 2020. Enligt metoden bedöms verksamhetens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Den genomsnittliga mognadsgraden är baserat på snittet av mognadsgraden för de respektive 12 områdena.

Baserat på den analys och granskning som genomförts bedöms Västerås stad ha den genomsnittliga mognadsgraden 3,1 av 5,0. 3,1 är en något lägre mognadsgrad än vad EY rekommenderar för en kommun, givet den stora mängd personuppgifter och känsliga personuppgifter som hanteras inom förvaltningarna, men något högre än vad EY generellt observerar för kommuner.

- Kommunen har lagt mycket resurser på arbetet med informationssäkerhet vilket avspeglas i ett en väl utvecklad organisation och rutiner. Kunskapsnivån inom dataskyddsorganisationen är hög och de ansvariga arbetar överlag strukturerat med dataskyddsfrågor. Således bedöms mognadsgraden vara högst inom organisation och ansvar, samt de två rutintunga områdena behandling av personuppgifter och riskhantering.
- Rapportens huvudsakliga iakttagelse berör området kontroll. Kommunens granskning och rapportering inte har utvecklats i samma takt som övrigt arbete och i dagsläget saknas granskning av förvaltningarnas arbete med personuppgiftssäkerhet i stort sett helt. Det finns varken internkontroller inom förvaltningarna som tydligt täcker in de olika aspekterna av dataskyddsarbetet, eller granskningar från centralt håll. Detta bidrar till att den faktiska efterlevnaden av rutiner för personuppgiftshantering är oklar.
- Verksamheten bör införa kontrollrutiner, där granskningar för personuppgiftshantering genomförs regelbundet och rapportering sker mellan förvaltningarna, dess nämnder, DSO och kommunledningen. Genom att införa mer strukturerade analyser och åtgärdsplaner kommer även arbetet inom övriga områden förbättras ytterligare.
- EY rekommenderar vidare att kommunen inför regelbundna utbildningsinsatser inom GDPR samt att de mest kritiska verksamheterna tydliggör sin strategi för utbildningsinsatser och medvetenhet hos sina medarbetare och inför åtgärder därefter.
- EY har även genomfört en separat granskning av kommunens bolagskoncern. Anmärkningsvärt är att Västerås stad trots helägarskap i flera av bolagen inte i en betydande grad har samordnat arbetet med personuppgiftssäkerhet med bolagen.

Revisionen har överlämnat revisionsrapporten till kommunfullmäktige. Rapporten är publicerad på stadens hemsida www.vasteras.se
För ytterligare information, kontakta revisionens ordförande Asta Matikainen Lecklin tfn: 076-896 43 86 eller revisionssamordnare Christel Modin tfn: 076-569 48 43.

Oktober 2020