2020-11-09

TJÄNSTESKRIVELSE
KFKS 2020/860

Kommunstyrelsen

Revisionsrapport nr 2 2020 - Granskning av efterlevnad Dataskyddsförordningen GDPR

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen fatta följande beslut.

Kommunstyrelsen antar förslaget yttrande över revisionsrapport 2/2020 enligt bilaga 3 till tjänsteskrivelse daterad den 9 november 2020.

Sammanfattning

De förtroendevalda revisorerna har under våren 2020 låtit EY genomföra en granskning av efterlevnaden av den allmänna dataskyddsförordningen (dataskyddsförordningen, GDPR) inom kommunen i stort. Av den sammanfattande bedömningen framgår att revisorerna bedömer att efterlevnaden av dataskyddsförordningen i allmänhet är god, men att den behöver stärkas inom vissa områden. Framförallt består de identifierade bristerna av avsaknad av formaliserade rutiner för uppföljning och kontroll av efterlevnad.

Ärendet

Då Nacka kommun med dess verksamheter hanterar stora mängder personuppgifter, har de förtroendevalda revisorerna beslutat att under våren 2020 genomföra en granskning av efterlevnaden av dataskyddsförordningen för kommunen som helhet.

Revisorernas synpunkter och rekommendationer utifrån granskningen

Av den sammanfattande bedömningen framgår att revisorerna bedömer att efterlevnaden av dataskyddsförordningen generellt sett är god jämfört med andra kommuner. Utifrån den stora mängden personuppgifter och dess känslighet, ligger kommunens hantering till stor del i linje med EY:s rekommendationer i området. Den högsta mognadsgraden observeras inom organisation och ansvar, utbildning samt riskhantering. Utbildningsinsatser och metoder för riskanalys och konsekvensbedömning är väl utvecklade. Något lägre mognad finns inom styrande dokument, som behöver uppdateras enligt kraven i dataskyddsförordningen och eventuellt utformas tydligare. Den förbättringspunkten som

EY tycker ska prioriteras är dock kontroll. Det föreslås en fastslagen granskningsplan som tydliggör uppföljning och konsekvenser, med åtgärdsplaner godkända av ledningen. Det rekommenderas även att kommunen fastslår rapporteringskrav till styrelsen för att säkerställa att efterlevnad av dataskyddsförordningen dokumenteras och rapporteras till ledningsnivå.

Utifrån granskningens resultat rekommenderar revisorerna att kommunstyrelsen:

- Utöka kontrollen av efterlevnad genom centralt förankrade granskningar med tillhörande åtgärdsplaner godkända av ledningen.
- Uppdaterar styrdokument enligt kraven i dataskyddsförordningen där så är lämpligt, exempelvis styrdokument för kontroll av efterlevnad och inbyggt dataskydd.
- Utvärderar kommunens processer inom personuppgiftshantering utifrån grad av centralisering och decentralisering för att bedöma om varje process är optimal ur ett resursperspektiv.
- Prioriterar att kontrollera kvalitéten av registerutdrag.

Kontroller

I granskningen uttalas att Nacka kommun har kommit långt i implementationen av rutiner för säker hantering av personuppgifter. Det föreslås dock att kommunen inom ramen för den interna kontrollen antar en granskningsplan med stickprovskontroller för att identifiera och följa upp brister. Stickprovskontroller föreslås för registerförteckning, registerutdrag, gallring, konsekvensbedömning, informationsklassning och personuppgiftsbiträdesavtal.

Styrande dokument

I granskningen föreslås att styrande dokument uppdaterade och tillsammans bildar en logisk och tydlig kedja av beslut, ansvar och instruktioner. Det föreslås också att informationssäkerhetsstrategin uppdateras i enlighet med dataskyddsförordningen.

Centralisering och effektivitet

I granskningen föreslås att Nacka kommun utvärderar graden av centralisering respektive decentralisering för att optimera resursfördelningen. EY tillstår att Nacka redan arbetar med detta inom digitaliseringsfrågor och rekommenderar att Nacka fortsätter med detta arbete.

Begäran från registrerade

Granskningen har visat att processen för registerutdrag är förhållandevis komplex och medför en svårbedömd risk för fel. Det rekommenderas att involvera digitaliseringsenheten och undersöka potentiell förenkling och automatisering av processen.

Förslag på yttrande i korthet

Av förslaget till yttrande framgår att kommunen, i likhet med revisorernas bedömning, konstaterar att kommunen kommit långt i den praktiska implementationen av rutiner för en säker hantering av personuppgifter. Denna implementation utgör en viktig förutsättning för att kommunen ska kunna följa upp efterlevnaden av dataskyddsförordningen. Det framgår även att kommunen, utifrån reglementet för intern kontroll, har goda förutsättningar att

kontrollera efterlevnaden av dataskyddsförordningen om det bedöms finnas risker i hanteringen. I förslaget till yttrande lyfts även bland annat styrdokumenten inom området är i behov av en översyn och att ett sådant arbete redan pågår.

Ekonomiska konsekvenser

Genom exempelvis automatisering av processen för registerutdrag och annan effektivisering kan arbetstidsbesparingar uppstå, vilket kan innebära att ekonomiska medel används på ett kostnadseffektivare sätt. Bristande efterlevnad av dataskyddsförordningen kan även innebära att kommunen blir föremål för sanktionsavgifter och skadeståndskrav.

Konsekvenser för barn

Barns personuppgifter anses vara extra skyddsvärda i dataskyddsförordningen. En grundläggande förutsättning för att värna om barns integritet och privatliv är genom god efterlevnad av dataskyddsförordningen och en hög nivå av informationssäkerhet.

Bilagor

1. Revisionsskrivelse – Granskning. Efterlevnad av Dataskyddsförordningen GDPR (daterad den 16 september 2020)
2. Revisionsrapport nr 2 2020 – Granskning av efterlevnad Dataskyddsförordningen GDPR (daterad den 16 juni 2020)
3. Förslag till yttrande

Hans-Otto Halvorsen
Stöd- och servicedirektör
Stadsledningskontoret

William Höglund
Dataskyddsombud
Juridik- och kanslienheten