KS § 388

Granskning om efterlevnad av dataskyddsförordningen (GDPR) - yttrande till kommunfullmäktige

Diarienummer: 2021/304

Sammanfattning av ärendet

Ernst & Young AB (EY) har på uppdrag av de förtroendevalda revisorerna genomfört en granskning av kommunens nämnder, med kommunstyrelsen som ansvarig nämnd, med avseende på personuppgiftshantering. Granskningen syftade till att ge en *övergripande* förståelse av huruvida Västerviks kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Kommunens revisorer har i skrivelse 15 september 2021 överlämnat rapporten till kommunstyrelsen och lämnat ett antal övergripande rekommendationer. Rekommendationer har också lämnats till de kommunala bolagen som lämnar egna svar på rapporten.

Förslag till beslut

Kommunstyrelsen föreslår kommunfullmäktige besluta
att godkänna de redovisade svaren på revisionsrapporten om granskning av efterlevnad dataskyddsförordningen (GDPR).

Kommunstyrelsen föreslår kommunfullmäktige besluta

att godkänna de redovisade svaren på revisionsrapporten om granskning av efterlevnad dataskyddsförordningen (GDPR).

Beslutet är elektroniskt justerat.

Beslutet skickas till

Kommunfullmäktige

Handlingar i ärendet

Kommunstyrelsens förvaltnings skrivelse 30 november 2021
Västerviks Kraft Elnät ABs yttrande 2021-10-25, § 103
Västervik Miljö & Energi ABs yttrande 2021-10-25, § 153
Revisorernas granskningsrapport 15 september 2021

VÄSTERVIKS KOMMUN

Kommunstyrelsens förvaltning
Enheten för räddningstjänst och samhällsskydd

Diarienr: 2021/304
Tjänsteskrivelse

2021-11-30

Informationssäkerhetssamordnare
Anna Grandalen
0490-25 57 52
anna.grandalen@vastervik.se

Kommunstyrelsen

Granskning av efterlevnad av dataskydds-förordningen - svar

Sammanfattning

Ernst & Young AB (EY) har på uppdrag av de förtroendevalda revisorerna genomfört en granskning av kommunens nämnder, med kommunstyrelsen som ansvarig nämnd, med avseende på personuppgiftshantering. Granskningen syftade till att ge en *övergripande* förståelse av huruvida Västerviks kommun bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Kommunens revisorer har i skrivelse 15 september 2021 överlämnat rapporten till kommunstyrelsen och lämnat ett antal övergripande rekommendationer. Rekommendationer har också lämnats till de kommunala bolagen som lämnar egna svar på rapporten.

Bakgrund och beskrivning

Granskningen syftade till att svara på tre revisionsfrågor:

- Arbetar Västerviks kommun ändamålsenligt för att uppfylla de krav och regleringar för personuppgiftshantering som har införts i och med dataskyddsförordningen (GDPR)?
- Är Västerviks kommuns policyer och riktlinjer ändamålsenliga för att uppnå regelefterlevnad med avseende på dataskyddsförordningen (GDPR)?
- Har Västerviks kommun ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen (GDPR)?

Övergripande rekommendationer lämnas inom följande områden:

- Styrning och styrande dokument,
- Granskning och rapportering,
- Riskhantering,
- Utbildning och medvetenhet.

Förvaltningens beredning och svar rapporten

Enligt rapporten har granskning gjorts av kommunens nämnder med kommunstyrelsen som ansvarig nämnd. Förvaltningen vill förtydliga att kommunstyrelsen inte är ansvarig för eller överordnad övriga nämnder mer än genom den så kallade uppsiktsplikten. Den innebär att kommunstyrelsen ska ha uppsikt över nämndernas verksamhet. Uppsiktsplikten fullgörs bland annat genom de månatliga månadsrapporterna, delårsrapporter, årsbokslut, dialogmöten och genom nämndernas redovisning av sin internkontroll.

Det bör förtydligas att varje nämnd är personuppgiftsansvarig enligt dataskydds-förordningen och ansvarar därmed för de personuppgifter som hanteras inom nämndens verksamhet. Det innebär att nämnderna också ansvarar för att säkerställa nödvändig uppföljning av arbetet och avgör hur denna ska ske.

En del av de rekommendationer som lämnas i rapporten handlar om att ta fram övergripande och gemensamma rutiner för arbetet med dataskyddsfrågor. Det är förvaltningens bedömning att det är positivt med gemensamma styrdokument och rutiner för att underlätta arbetet med att följa dataskyddsförordningen i kommunens olika verksamheter.

Ett förslag till handlingsprogram utifrån de föreslagna övergripande rekommendationerna har tagits fram och redovisas i bilaga till denna skrivelse. Där framgår vilka åtgärder som planeras utifrån varje rekommendation.

Ekonomi och resursbehov

För att fullfölja handlingsplanen krävs personella resurser. Dessa bedöms inrymmas i befintliga resurser.

Barnperspektivet

Ärendet bedöms i detta läge inte påverka barn.

MBL-förhandling

MBL-förhandling är inte nödvändigt i ärendet.

Uppföljning och utvärdering

Beslutet bedöms inte behöva särskild uppföljning eller utvärdering.

Förslag till beslut

Kommunstyrelsen föreslår kommunfullmäktige besluta

att godkänna de redovisade svaren på revisionsrapporten om granskning av efterlevnad dataskyddsförordningen (GDPR).

Anders Björlin
Kommundirektör

Ulf Kullin
Förvaltningsledare

Joakim Jansson
Räddnings- och säkerhetschef

Bilagor

Handlingsplan 30 november 2021 utifrån EY:s granskning av efterlevnad av dataskyddsförordningen

Beslutet skickas till

Kommunfullmäktige

Bilaga 1
Handlingsplan utifrån EY:s granskning av efterlevnad av dataskyddsförordningen (GDPR)

Övergripande rekommendationer och förslag på åtgärder			
Styrning och styrande dokument	**Svar**	**Ansvarig för att leda arbetet enligt svar**	**Tidsperiod/klart**
1. Upprätta en övergripande informationssäkerhetspolicy	En informationssäkerhetspolicy tas fram. Koncernens informationssäkerhetsgrupp tar fram förslag som sedan behandlas i KLG, KS och KF.	Informationssäkerhetssamordnare	2022
2. Upprätta riktlinjer och anvisningar för dataskyddsarbetet utifrån policyn och som täcker in alla relevanta delar inom förordningen.	Koncernens informationssäkerhetsgrupp tillsammans med dataskyddsombud tar fram förslag som sedan behandlas i KLG.	Informationssäkerhetssamordnare	2022
3. Etablera en rutin för uppföljning av kommunens nämnder, för att säkerställa att nämnder efterlever den policy och de regler som fastställts.	Informationssäkerhetssamordnare stämmer av med ansvarig för internrevision hur uppföljning kan ske inom befintliga strukturer. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
Granskning och rapportering	**Svar**	**Ansvarig**	**Tidsperiod/klart**
1. Implementera en granskningsplan för att utvärdera och säkerställa att alla verksamheter lever upp till relevanta krav inom personuppgiftshantering.	I lagen beskrivs dataskyddsombudets uppdrag för att övervaka efterlevnaden av förordningen). Tillsammans med dataskyddsombud tas ett förslag fram på hur arbetet kan ske i linje med aktuell lagstiftning. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
2. Etablera en formell rutin för verksamheterna att dokumentera och	Varje nämnd ansvarar själv för hur rapportering ska ske. Tillsammans med dataskyddsombuden tas förslag på rutin fram. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022

kontinuerligt rapportera resultatet av GDPR-arbetet till ledningsnivå på kommunen.			
3. Fastslå ett rapporteringskrav gällande frekvens och innehåll som rapportering till kommunstyrelsen ska utgå från.	Bedömningen är att kommunstyrelsen inte behöver fastställa ett rapporteringskrav från nämnderna. Vid det årliga ärendet om internkontroll finns möjlighet att lyfta behovet av ytterligare kontroller. Varje nämnd ansvarar för hur rapportering av arbetet ska ske.	Informationssäkerhetssamordnare	2022
Riskhantering	**Svar**	**Ansvarig**	**Tidsperiod/klart**
1. Etablera en metod samt en rutin för att bedöma risker i personuppgiftsbehandlingen.	Ta fram en metod och rutin tillsammans med koncernens informationssäkerhetsgrupp och dataskyddsombud. Detta synkroniseras med befintliga metoder inom andra områden. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
2. Att samtliga nämnder implementerar rutiner samt ansvarsfördelning som säkerställer att konsekvensbedömningar utförs i så fall då riskanalyserna visar på hög integritetsrisk för den registrerade.	Ta fram rutin samt ansvarsfördelning tillsammans med koncernens informationssäkerhetsgrupp och dataskyddsombud. Därefter behandling i KLG	Informationssäkerhetssamordnare	2022
3.Genomför konsekvensbedömningar inför varje ny behandling av personuppgifter inom verksamheten, samt vid regelbundna tillfällen.	Ta fram en instruktion för nya behandlingar av personuppgifter tillsammans med koncernens informationssäkerhetsgrupp och dataskyddsombud. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
Utbildning och medvetenhet	**Svar**	**Ansvarig**	**Tidsperiod/klart**
1. Implementera en utbildnings- och informationsplan som inkluderar regelbundna interna utbildningar	Ta fram en utbildnings- och informationsplan tillsammans med koncernens informationssäkerhetsgrupp och dataskyddsombud. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
2. Implementera en rutin för regelbunden uppföljning för att säkerställa att alla anställda tar del av utbildningarna.	Ta fram en utbildnings- och informationsplan tillsammans med koncernens informationssäkerhetsgrupp och dataskyddsombud. Därefter behandling i KLG.	Informationssäkerhetssamordnare	2022
3. Etablera en rutin för att kontinuerligt uppdatera utbildningsmaterial för att säkerställa att alla anställda inom verksamheten är medvetna om dataskyddsförordningens krav på personuppgiftshantering.	Koncernens informationssäkerhetsgrupp och dataskyddsombud arbetar in rutiner för att uppdatera utbildningsmaterial i utbildnings- och informationsplanen som ska tas fram.	Informationssäkerhetssamordnare	2022