

§ 153

Remiss efter granskning av efterlevnad av dataskyddsförordningen (GDPR)

Diarienummer: 2021/74

Bakgrund

Ernst & Young AB (EY) har på uppdrag av lekmannarevisorerna genomfört en granskning av Västervik Miljö & Energi AB (VMEAB) samt Västerviks Kraft Elnät AB (VKEN), med avseende på personuppgiftshandling. Granskningen syftade till att ge en *övergripande* förståelse av huruvida de båda bolagen bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshandling gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden, vilka bedömts på en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms VMEAB ha en genomsnittlig mognadsgrad på 2,79 av 5,00. Mognadsgraden är en genomsnittlig mognadsgrad jämfört med vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är dessutom en siffra i linje med vad EY anser kan förväntas av bolaget, givet den ringa mängd känsliga personuppgifter som hanteras.

Mot bakgrund av granskningens iakttagelser rekommenderas VMEAB att:

Granskning

- Vidareutveckla den interna kontrollen avseende personuppgiftshandling och implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att relevanta krav på personuppgiftshandlingen uppfylls.

Utbildning

- Etablera en rutin för att kontinuerligt utbilda anställda inom dataskyddsförordningen.
- Implementera rutiner som säkerställer att internutbildningar uppdateras över tid.

Hantering av leverantörsrelationer

- Arbeta vidare för att upprätta PUB-avtal med alla leverantörer där det är relevant.
- Upprätta en dokumenterad rutin för att regelbundet granska personuppgiftsbiträden.

Förslag till beslut

Att VMEAB inom 12 månader dock senast 2022-10-31 genomför relevanta åtgärder inom de tre rekommenderade åtgärdsområdena granskning, utbildning samt hantering av leverantörsrelationer.

Styrelsen beslutar

I enlighet med förslaget till beslut.

§ 153 fortsättning

Beslutet skickas till

Västerviks kommuns lekmannarevisorer

Handlingar i ärendet

Missiv från kommunens lekmannarevisorer

Rapport från EY – Granskning av efterlevnad GDPR

KMA-ansvarig, Ansvarig fysisk säkerhet
Rickard Wester
0490 - 25 70 61
rickard.wester@vastervik.se

Styrelsen för Västervik Miljö & Energi AB

Remiss efter granskning av efterlevnad av dataskyddsförordningen (GDPR)

Ernst & Young AB (EY) har på uppdrag av lekmannarevisorerna genomfört en granskning av Västervik Miljö & Energi AB (VMEAB) samt Västerviks Kraft Elnät AB (VKEN), med avseende på personuppgiftshantering. Granskningen syftade till att ge en *övergripande* förståelse av huruvida de båda bolagen bedriver ett ändamålsenligt arbete med dataskyddsförordningen (the General Data Protection Regulation, GDPR) och i vilken utsträckning som de åtgärder som förordningen stipulerar uppfylls.

Granskningen utgår från EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter. Ramverket består av 12 områden, vilka bedömts på en skala från 1 (*begynnande*) till 5 (*optimerad*).

Baserat på den analys och granskning som genomförts bedöms VMEAB ha en genomsnittlig mognadsgrad på 2,79 av 5,00. Mognadsgraden är en genomsnittlig mognadsgrad jämfört med vad EY generellt observerar i en offentlig verksamhet av liknande storlek och karaktär. Det är dessutom en siffra i linje med vad EY anser kan förväntas av bolaget, givet den ringa mängd känsliga personuppgifter som hanteras.

Mot bakgrund av granskningens iakttagelser rekommenderas VMEAB att:

Granskning

- Vidareutveckla den interna kontrollen avseende personuppgiftshantering och implementera en granskningsplan för att kontinuerligt utvärdera och säkerställa att relevanta krav på personuppgiftshantering uppfylls.

Utbildning

- Etablera en rutin för att kontinuerligt utbilda anställda inom dataskyddsförordningen.
- Implementera rutiner som säkerställer att internutbildningar uppdateras över tid.

Hantering av leverantörsrelationer

- Arbeta vidare för att upprätta PUB-avtal med alla leverantörer där det är relevant.
- Upprätta en dokumenterad rutin för att regelbundet granska personuppgiftsbiträden.

Bakgrund och beskrivning

Den aktuella granskningen är en del av en större granskning, där samtliga kommunala bolag och förvaltningar undersökts på motsvarande sätt. Varje bolag respektive förvaltningskommunen har fått egna resultatrapporter med rekommenderade åtgärder.

Den del av rekommenderade åtgärder som kan vara lämplig att genomföra i samverkan inom hela kommunkoncernen är utbildningar. Då det gäller övriga åtgärder ser behovet olika ut i respektive förvaltning och bolag.

Förutom de tre områdena där åtgärder rekommenderas, finns i EY:s rapport ytterligare ett antal noteringar. På dessa punkter kommer VMEAB att bedriva ett långsiktigt förbättringsarbete

Bolagets beredning

Förslaget till svar på remissen från kommunens lekmannarevisorer har tagits fram av KMA-enheten i samverkan med bolagets VD.

Förslag till beslut

Att VMEAB inom 12 månader dock senast 2022-10-31 genomför relevanta åtgärder inom de tre rekommenderade åtgärdsområdena granskning, utbildning samt hantering av leverantörsrelationer.

Per Allerth
Vd

Rickard Wester
Kvalitets- och miljöansvarig

Bilagor

Missiv från kommunens lekmannarevisorer
Rapport från EY – Granskning av efterlevnad GDPR

Beslutet skickas till

Västerviks kommuns lekmannarevisorer