Upplands-Bro kommun
Revisorerna

Revisionsskrivelse 2019-12-10

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Granskning av efterlevnad till dataskyddsförordningen GDPR

På vårt uppdrag har EY genomfört en granskning av kommunens och Upplands-Brohus hantering av personuppgifter. Granskningens syfte har varit att ge en övergripande förståelse av huruvida Upplands-Bro kommun och Upplands-Brohus bedriver ett ändamålsenligt arbete med dataskyddsförordningen (The General Data Protection Regulation, GDPR) och hur kommunens mognad ser ut i uppfyllelse av de åtgärder som förordningen stipulerar.

EY:s övergripande bedömning är att Upplands-Bro kommun har en förhållandevis låg mognadsgrad jämfört med andra offentliga organisationer av liknande storlek i förhållande till antal anställda och övergripande verksamhet. Mognadsgraden bedöms vara som högst inom information till registrerade och inbyggt dataskydd. Lägst är mognadsgraden inom kontroll, styrning, riskhantering och hantering av leverantörsrelationer.

Kommunens största och viktigaste förbättringspunkter ligger i att upprätta en formaliserad och informationssäkerhetsspecifik organisationsstruktur med tillhörande roller, tydlig ansvarsfördelning. Majoriteten av styrdokument och policys är utdaterade och bör uppdateras för att sätta en struktur i kommunens dataskyddsarbete. Kommunen bör även arbeta proaktivt med riskhantering och upprätta personuppgiftbiträdesavtal med leverantörer för att minska risker för integritetsincidenter och ogiltig behandling av personuppgifter inom sina verksamheter såväl som hos leverantörer. Vidare finns ett behov av att införa styrande rutiner och processer för granskning och uppföljning inom i stort sett samtliga av de 12 undersökta områdena, både för kommunen i helhet och för Upplands-Brohus. Slutligen behöver Upplands-Brohus utföra en analys om ett eget dataskyddsombud behövs och dokumentera ett beslutagande. Utan detta bedömer EY att det kommer bli svårt att skapa tillfredsställande förutsättningar för att bedriva ett ändamålsenligt arbete med personuppgiftshantering på både kort och lång sikt inom kommunen.

Vi rekommenderar att kommunstyrelsen:

- Uppdaterar informationssäkerhetspolicyn så att den beskriver syftet med kommunens dataskyddsarbete och innehåller en strategi för kommunens informationssäkerhetsarbete.
- Implementerar en rutin för att följa upp att verksamheterna efterlever de regler och policys som är fastställda i informationssäkerhetspolicyn.
- Fastställer en formell, informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning för att undvika överarbetsbelastning och personberoende.
- Fastställa en åtgärdsplan inkluderande tidsplan och ansvarig person för att åtgärda eventuella gap där dataskyddsförordningen inte efterlevs.
- Implementera en granskningsplan för att utvärdera och säkerställa att kommunen uppfyller relevanta krav på hantering av personlig information, exempelvis som del i arbetet med intern kontroll.

- Inventerar samtliga IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer, i syfte att slutföra arbetet med att ingå personuppgiftsbiträdesavtal med externa leverantörer.
- Tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till kommunens användare med en bestämd frekvens.
- Följer upp att den obligatoriska utbildningen av nyanställda slutförs samt inför vidareutbildning och uppföljning av befintliga medarbetares deltagare.

Utförligare förklaring till rekommendationerna finns i granskningsrapporten avsnitt 2.2.

Vi rekommenderar att styrelsen för Upplands-Brohus:

- Genomför en analys och tar ett beslut gällande om bolaget behöver ett dataskyddsombud. Om inget ombud anses nödvändigt, ska dennes ansvarsområden fördelas vidare till andra personer i dataskyddsorganisationen.
- Tar fram och dokumenterar en formell informationssäkerhetsspecifik organisationsstruktur med tillhörande roller och tydlig ansvarsfördelning.
- Dokumenterar rutiner och processer beträffande hantering av personuppgifter i styrdokument som är i linje med dataskyddsförordningens krav.
- Fastställer en granskningsplan för att utvärdera och säkerställa att man uppfyller relevanta krav på hantering av personlig information och efterlever de rutiner som har implementerats.
- Utför en inventering av samtliga IT-system och tjänster som behandlar personuppgifter och som tillhandahålls till leverantörer och sedan upprättar personuppgiftsbiträdeskontrakt med alla berörda leverantörer.

Utförligare förklaring till rekommendationerna finns i granskningsrapporten avsnitt 2.3.

Vi önskar svar från kommunstyrelsen och bolagsstyrelsen senast 2020-03-24.

För Revisorerna i Upplands-Bro kommun

Roger Gerdin

Thomas Ljunggren

Bilaga: Revisionsrapport nr 5/2019 – Granskning av efterlevnad till dataskyddsförordningen GDPR