

KOMMUNSTYRELSEN

Dnr KSF 2021/196

§ 17 Dataskyddsbud och cybersäkerhet

Beslut

Kommunstyrelsen beslutar:

1. Avtalsförslag från Sydarkivera godkänns och ska anses träda i kraft retroaktivt från och med 2022-01-01.
2. Beslutet finansieras genom ianspråkstagande av 125 000 kr från kommunstyrelsens konto till förfogande 2022, därefter ska kostnaden inarbetas i budgeten.
3. Nämnderna uppmanas att utse förbundsjurist Therese Jigsved till dataskyddsbud.
4. Kommundirektören tillförs 400 000 kr från kommunstyrelsens konto till förfogande 2022 för att kunna stärka kommunens arbete med cybersäkerhet genom att tillsätta en informationssäkerhetsansvarig. Därefter ska kostnaden inarbetas i budgeten.

Ärendebeskrivning

Sammanfattning

På uppdrag av kommunstyrelsen har förvaltningen tagit fram förslag på nytt dataskyddsbud genom kommunalförbundet Sydarkivera. Samtidigt har Unikom uppmärksammat samtliga ägarkommuner på vikten av Cybersäkerhet. Förvaltningen har tillskapat en enhet som ska arbeta med digitaliserings- och IT-utveckling för att driva på förvaltningens arbete med digitalisering, se ärende om Digitaliseringsstrategi. Det saknas dock tillräckliga resurser för att kunna genomföra det utvecklande arbete som krävs för en god cybersäkerhet vilket inkluderar informationssäkerhet och arbete enligt GDPR.

Därför föreslås en förstärkning som innebär att medel tillförs så att förbundsjurist Therese Jigsved, Sydarkivera, kan utses som dataskyddsbud och förvaltningen tillförs medel motsvarande en halvtid som aktivt kan samordna och driva det interna arbetet för cybersäkerhet. Ett dataskyddsbud är en typ av tillsynsfunktion och stödfunktion, dataskyddsbudet ersätter inte en intern organisation som arbetar med GDPR i verksamheterna.

Cybersäkerhet består av Informationssäkerhet och IT-säkerhet

Arbete med cybersäkerhet handlar om hantering av interna och externa hot mot verksamhetskritiska informationstillgångar och IT-tjänster. God hantering uppnås genom ett strukturerat arbetssätt (styrmodell) för IT- och informationssäkerhetsaktiviteter. Som kommun krävs en högre grad av kontroll över vår IT- och informationssäkerhet än vad vi haft behov av tidigare. I en tid av digitalisering fungerar IT, teknik och data inte längre bara stödjande till verksamhetsprocesser, utan som drivare av dem. Misslyckande med att hantera IT- eller informationssäkerhetskrav kan få stora konsekvenser inte bara i de

KOMMUNSTYRELSEN

fall det utgör lagbrott (såsom GDPR), utan även i förlorat förtroende och tillit från våra medborgare. Hur allvarliga konsekvenserna blir beror till stor grad på hur bra man organiserat arbetet med sin cybersäkerhet, det vill säga IT- och informationssäkerhet.

Ett strukturerat förhållningssätt till IT- och informationssäkerhet innebär att ha kunskap om:

- IT-infrastruktur och applikationer (hårdvara och mjukvara) - förstå vilka av dessa som är kritiska och därmed särskilt skyddsvärda
- Informationstillgångar - förstå var de finns och vilken information som är känslig/kritisk och därmed särskilt värdefull

Baserat på förståelsen lokaliseras risker. Det handlar inte nödvändigtvis om att ta itu med alla risker, utan att göra ett välgrundat urval av vilka risker som ska hanteras, hur man gör det och vem som är ansvarig.

Informationssäkerhetsansvarigs ansvarsuppgifter, se bildspel om cybersäkerhet.

Dataskyddsombudets ansvarsuppgifter, se bildspel om information om DSO-tjänsten och Rapport om Sydarkiveras anslutande tjänster.

Beslutsunderlag

1. TjänsteskrivelseDSOoCybersäkerhet.pdf
2. Cybersäkerhet.pptx
3. Information om DSO-tjänsten 2021.pdf
4. Avtal om gemensamt dataskyddsombud med Höors kommun.pdf
5. Kommunstyrelsen 2021-10-26 (2021-10-26 KS §213).doc.pdf
6. Rapport Sydarkiveras anslutande tjänster.pdf
7. Kommunstyrelsens Arbetsutskott 2021-12-14 (2021-12-14 KSAU §322).doc.pdf