



Handläggare  
Malin Johansson  
malin.johansson@bracke.se

Mottagare  
Kommunstyrelsen

## Medel till informationssäkerhetssamordnare

### Stabens förslag till beslut

Kommunstyrelsen beviljar medel till en tjänst som informationssäkerhetssamordnare med 700 000 kronor i 2026 års nivå.

### Sammanfattning av ärendet

Staben föreslår att en tjänst som informationssäkerhetssamordnare inrättas, då det saknas resurser och tjänst för ett systematiskt informationssäkerhetsarbete. Den nya cybersäkerhetslagen (baserad på NIS2-direktivet) som träder i kraft 2026 ställer höga krav på kommunens informationssäkerhetsarbete, inklusive incidentrapportering, riskhantering och ledningsansvar. Utan en samordnare riskerar kommunen sanktioner och sämre beredskap vid cyberangrepp. Tjänsten bör även inkludera dataskyddsuppgifter (GDPR) och signalskydd för att skapa helhet.

### Beskrivning av ärendet

#### Bakgrund

Staben föreslår att det ska inrättas en tjänst som informationssäkerhetssamordnare. Information är en av kommunens mest viktiga resurser. Informationssäkerhet handlar om att skydda information och säkerställa att informationstillgångar finns tillgängliga när de behövs, att de är korrekta, och att obehöriga inte får åtkomst till dem.

Bräcke kommun har hittills inte haft en tjänst som informationssäkerhetssamordnare utan arbetsuppgifter kopplat till informationssäkerhet har delats mellan funktionerna säkerhetssamordnare, IT-samordnare samt kommunsekreterare. Ingen av ovanstående funktioner har utrymme för detta arbete i sina tjänster och därmed har arbetet med informationssäkerhet blivit bristande.

Krav och behov inom området informationssäkerhet och dataskydd har ökat under de senaste åren och kommer fortsätta öka. Ny lagstiftning ställer också högre krav på informationssäkerhetsarbete. Berörda organisationer måste införa systematiskt informationssäkerhetsarbete och kan drabbas av sanktionsavgifter vid bristande efterlevnad.



Omvärldsutvecklingen visar på en ökning av cyberangrepp riktade mot offentliga aktörer, vilket i värsta fall kan leda till allvarliga driftstörningar, röjd information och skadat förtroende. En incident i närtid är angreppet på Miljödata AB, som är kommunens leverantör av personalsystem.

## Ny cybersäkerhetslagstiftning

En ny cybersäkerhetslag beräknas träda i kraft 15 januari 2026. Den ställer högre krav på kommunernas informationssäkerhetsarbete. Den föreslagna lagen *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* är Sveriges genomförande av EU:s NIS2-direktiv. Lagen innebär att kommuner och andra offentliga aktörer som tillhandahåller samhällsviktig verksamhet omfattas av tydliga skyldigheter inom cybersäkerhet. NIS2 (Network and Information Systems Directive2) är en uppdatering av det tidigare NIS-direktivet. Syftet med NIS2 är att säkerställa en hög nivå av informationssäkerhet i hela EU genom att stärka skyddet av samhällsviktiga tjänster som en följd av den ökade digitaliseringen och hotbilden av cyberhot.

Kommunstyrelsens ledamöter samt ett antal personer från tjänsteorganisationen fick i början av juni en utbildning i och introduktion till NIS2. Den innehöll en genomgång av direktivet och om hur kommunen påverkas.

Det finns även ett direktiv från EU som kallas CER-direktivet (Directive on the resilience entities) som ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet. När lag, förordning och föreskrifter finns börjar förordningen gälla i Sverige.

Kraven på informationssäkerhetsarbete har ökat de senaste åren och kommer öka ytterligare i och med anpassningar till NIS2-direktivet och ny lagstiftning. För Bräcke kommun innebär direktivet och den nya lagstiftningen:

- **Anmälningsskyldighet:** Kommunen behöver identifiera de delar av organisationen som omfattas av lagen och anmäla dessa till relevant tillsynsmyndighet.
- **Systematiskt riskarbete:** Kommunen blir skyldig att införa och underhålla ett riskbaserat arbetssätt med informations- och cybersäkerhet, inklusive återkommande risk- och sårbarhetsanalyser.
- **Säkerhetsåtgärder:** Tekniska och organisatoriska åtgärder ska införas för att förebygga, upptäcka och hantera incidenter. Krav ställs även på utbildning av ledning och i viss mån personal.



- **Incidentrapportering:** Betydande incidenter som påverkar kommunens nätverks- eller informationssystem ska rapporteras till tillsynsmyndighet inom fastställda tidsramar.
- **Tillsyn och sanktioner:** Kommunen kan bli föremål för tillsyn av myndighet och i förlängningen sanktioner eller avgifter om kraven inte uppfylls. Sanktionerna kan uppgå till 10 miljoner kronor och enskilda individer kan bli betalningsansvariga. Den administrativa sanktionsavgift som införs för offentlig förvaltning föreslås ligga på minst 5 000 kr och som mest 10 000 000 kr.
- **Ledningsansvar:** Kommunens ledning förväntas ta ett tydligare ansvar för cybersäkerhetsfrågor och säkerställa att tillräckliga resurser finns för att uppfylla lagens krav. Det innebär att ledningen har ett personligt ansvar och kan bli personligt ansvariga för sanktioner.

Att inrätta en tjänst som informationssäkerhetssamordnare är en nödvändig åtgärd för att kommunen ska kunna möta de kommande skyldigheterna. Funktionen blir central för att bygga upp rutiner för riskhantering, utbildning, incidentrapportering och samordning mellan verksamheterna.

Om staben inte tilldelas medel för att inrätta en tjänst som informationssäkerhetssamordnare kommer det inte vara möjligt att bedriva ett systematiskt och hållbart arbete med informationssäkerhetsfrågor.

## **Dataskydd bör samordnas med informationssäkerhet**

Tjänsten som informationssäkerhetssamordnare bör även innefatta uppgifter som har att göra med kommunens dataskydd. Informationssäkerhet handlar om att skydda all typ av information från obehörig åtkomst, förlust eller manipulation. Dataskydd enligt EU-direktivet General Data Protection Regulation (GDPR) handlar om att skydda personuppgifter – alltså en särskild typ av information. Båda områdena bygger på samma principer och att dela upp arbetet med uppgifterna riskerar därför att skapa dubbelarbete eller luckor i det strategiska arbetet med frågorna.

## **Signalskydd**

Dagens samhälle kräver robusta och säkra kommunikationer. Signalskydd kan användas för att skydda information från obehörig insyn och påverkan. Signalskyddssystem är avsedda att skydda säkerhetsskyddsklassificerade uppgifter när dessa ska kommuniceras. Det kan röra sig om uppgifter i pappersdokument, samtal, filer eller annan form av data som behöver skyddas. Att inkludera signalskydd i informationssäkerhetssamordnarens tjänst skulle innebära att kommunen tar höjd för samtlig informationsklassning, inklusive säkerhetsskyddsklassificerade uppgifter.



## Omvärldsbevakning

En aktuell omvärldsbevakning på arbetsförmedlingens platsbank visar på ett antal annonser från kommuner som söker informationssäkerhetssamordnare, ofta i kombination med arbete inom dataskydd.

I länet har kommunerna antingen tillsatt tjänster för ändamålet eller är i en intensiv process för att utreda hur de ska möta det nya uppdraget. Det har tidigare gjorts försök att hitta samverkansformer i länet men dessa har strandat både gällande informationssäkerhetssamordnare och dataskyddsombud.

Regeringen föreslår i budgetpropositionen för 2026 en satsning på nationell cybersäkerhet. Medlen ska fördelas mellan det nationella cybersäkerhetscentret (NCSC) samt kommuner och regioner. Förslaget i budgetpropositionen innehåller kompensation till kommuner och regioner för genomförandet av NIS2-direktivet och CER-direktivet med 200 miljoner kronor respektive 60 miljoner kronor per år till kommuner. Medlen är tänkta att tillföras via de generella statsbidragen och är avsedda att täcka kostnader för att möta de nya lagkraven på cybersäkerhet och motståndskraft i samhällsviktig verksamhet.

## Sammanfattande bedömning

Genom att samla uppgifter inom informationssäkerhet och dataskydd i en och samma tjänst skapas bättre förutsättningar för helhetssyn, samordning och prioritering. Det blir enklare att ta fram gemensamma riktlinjer, utbildningsinsatser och att arbeta med incidenthantering. Dessutom minskar risken för att GDPR-frågor hanteras reaktivt, vilket idag är en utmaning i kommunen. Mycket jobb kommer att behöva göras i verksamheterna, bland annat att klassificera information. Det behöver finnas en övergripande funktion som håller ihop arbetet och verkar för en korrekt och likartad hantering av frågor kopplade till informationssäkerhet och för att skapa bra förutsättningar för att leva upp till de nya lagkraven. Informationssäkerhet är inte bara teknik såsom servrar, byggnader och skalskydd. Det är också till exempel policies, strategier, kultur och attityder.

## Ekonomiska konsekvenser

En tjänst som informationssäkerhetssamordnare beräknas kosta 700 000 kr år 2026.

Bristande informationssäkerhet ökar risken för allvarliga incidenter, juridiska påföljder och eventuella sanktioner.



## Barnkonsekvensanalys

En stärkt informationssäkerhet för Bräcke kommun gynnar barn och unga genom att skyddet för deras personuppgifter och annan data bättre kan upprätthållas. Det bidrar även till att upprätthålla kontinuiteten i samhällsviktig verksamhet, såsom skola, förskola och socialtjänst. En samordnad hantering minskar risken för att barns integritet kränks och stärker tryggheten i kontakten med kommunen.

## Beslutsunderlag

Tjänsteskrivelse, 2025-10-01

## Beslutet skickas till

Staben

Malin Johansson  
Kommunsekreterare

Anders Lundin  
Kommundirektör

Camilla Samuelsson  
Stabschef