Tjänsteställe, handläggare
Juridik och Informationssäkerhet, Sofia Öhrman

Sammanträdesdatum
2024-01-30

Beteckning
Dnr: 23RS12327

Er beteckning:
4.1-107432/2023

Socialstyrelsen
Socialstyrelsen
106 30 Stockholm

# Svar på remiss avseende Socialstyrelsens förslag om föreskrifter för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn, 4.1-107432/2023

Region Örebro län, nedan regionen, har fått möjlighet att lämna synpunkter på Socialstyrelsens förslag om föreskrifter för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn.

NIS-lagen, som bygger på NIS-direktivet, trädde i kraft i augusti 2018. Det finns föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB) som kompletterar lagen. Syftet med den nu föreslagna föreskriften från Socialstyrelsen är att komplettera bestämmelserna 12-14 §§ NIS- lagen så att det blir tydligt för leverantörer vad som krävs av leverantörer för att de ska uppfylla dessa krav på säkerhetsåtgärder. Föreskriftsförslaget anger hur 12-14 §§ NIS-lagen ska tillämpas och omfattar sådana leverantörer som avses i 3 § NIS-lagen och som tillhandahåller samhällsviktiga tjänster inom sektorn hälso- och sjukvård. Vid implementeringen av NIS-direktivet överlät regeringen till tillsynsmyndigheterna och Socialstyrelsen att utforma denna typ av mer detaljerade föreskrifter.

Regionen lämnar härmed följande synpunkter på föreslagen föreskrift:

Regionen är positiv till att Socialstyrelsen kommer med förslag på föreskrift. Men då lång tid nu gått efter att NIS-lagen trätt i kraft och med beaktande av att NIS 2 direktivet ska börja att tillämpas i oktober 2024 kan det ifrågasättas om det inte är bättre att redan nu ta höjd för de förändringar som NIS 2

direktivet kommer att medföra. Dessutom kommer samtidigt det så kallade CER-direktivet som ska implementeras på ett samordnat sätt med NIS 2-direktivet. Hur kommer dessa båda direktiv att påverka innehållet i denna föreskrift?

I den föreslagna föreskriften står det i 5 § att leverantören ska, med utgångpunkt i 4 § om identifierade nätverk och informationssystem, upprätta en förteckning över dessa nätverk och informationssystem. Det finns en liknande reglering i ISO standarden 27002 punkten 5.9 ”Förteckning över information och andra relaterade tillgångar”. Här skiljer sig dock skrivningarna åt och det vore önskvärt om skrivningarna är mer enhetliga så att leverantörerna inte behöver ha flera olika förteckningar med delvis olika innehåll. Det noteras vidare att kravet på förteckningen medför ett omfattande arbete och det är inte tydligt vad detta medför för mervärde.

I 7 § framkommer att leverantören ska välja en riskanalysmetod som utgår från en etablerad standard. Valet av metod ska dokumenteras samt uppdateras kontinuerligt och uppgifterna ska bevaras i fem år från den tidpunkt den har tagits fram. En riskanalys är dagsfärsk och det föreslagna kravet på bevarande av riskanalys samt valet av metod i fem år framstår som onödigt och omotiverad. När det gäller val av standard så kan det vara en fördel att tydligt peka på ISO-standarden.

Regionen noterar vidare att vissa begrepp/benämningar i föreslagen föreskrift skiljer sig ifrån de begrepp som används i ISO-standarden. Exempelvis står det i föreskriften i 21 § om ”kontinuitetsplanering” medan begreppet ”kontinuitetshantering” ofta används i ISO-serien. Det är en fördel om samma begrepp och tillvägagångssätt används i föreskriften såsom i ISO-standarden.

För Region Örebro län

Andreas Svahn
Regionstyrelsens ordförande

Rickard Simonsson
Regiondirektör