Stockholms stad

PM Rotel IV (Dnr KS 2023/1350)

Anmälan om svar på remiss av Förslag till Socialstyrelsens föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn

Remiss från Socialstyrelsen

Förslag till beslut

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

Anmälan om svar på remiss godkänns.

Föredragande borgarrådet Alexander Ojanne

Sammanfattning av ärendet

Europaparlamentet och rådet antog 2016 det så kallade NIS-direktivet som 2018 införlivades i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. NIS-direktivet syftar till att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem, och därigenom förbättra den inre marknadens funktion. Socialstyrelsen fick vid införandet uppdrag att utfärda föreskrifter om säkerhetsåtgärder inom sektorn hälso- och sjukvård.

Socialstyrelsens förslag till föreskrifter innehåller bland annat krav på vad en riskanalys ska innehålla, grundläggande tekniska och organisatoriska åtgärder samt grundläggande åtgärder som leverantörer av samhällsviktiga tjänster inom hälso- och sjukvårdssektorn är skyldiga att vidta enligt NIS-lagen.

Socialstyrelsen har skickat föreskrifterna till bl.a. Stockholms stad för yttrande.

På grund av kort remisstid har staden svarat med stadsledningskontorets tjänsteutlåtande.

Beredning

Ärendet har remitterats till stadsledningskontoret, socialnämnden och äldrenämnden. Socialförvaltningen och äldreförvaltningen har inkommit med kontorsyttrande.

Stadsledningskontoret ställer sig positiv till Socialstyrelsens förslag till föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn och ser att de kommer stödja stadens systematiska informationssäkerhetsarbete. Stadsledningskontoret ser dock behov av vissa kompletteringar och förtydligande för att säkerställa syftet med föreskrifterna.

Socialförvaltningen är positiv men ser ett behov av ett antal förtydliganden för att säkerställa syftet med föreskrifterna.

Äldreförvaltningen välkomnar föreskrifterna och att ser de kommer att ge stöd i utformningen av det systematiska informationssäkerhetsarbetet.

Föredragande borgarrådets synpunkter

Jag föreslår att borgarrådsberedningen föreslår att kommunstyrelsen godkänner anmälan om svar på remiss.

Stockholm den 6 mars 2024

Alexander Ojanne

Bilaga

Remiss - Förslag till Socialstyrelsens föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn Dnr KS 2023/1350-1.1

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

Ärendet

Hälso- och sjukvårdens informationssäkerhetsarbete regleras till viss del genom patientdatalagen (2008:355), lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation samt Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Reglerna i dessa författningar riktar sig dock primärt till att skydda personuppgifter, inte själva informationssystemen som används för att upprätthålla den samhällsviktiga tjänsten.

Enligt NIS-lagen ska leverantörer av samhällsviktiga tjänster bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster. Mer detaljerade föreskrifter om hur kravet på ett systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas återfinns i MSB:s föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster. Enligt uppgift från Inspektionen för vård och omsorg (IVO) har cirka 240 leverantörer av samhällsviktiga tjänster inom hälso- och sjukvård anmält att de omfattas av NIS.

I föreskriften framgår att med samhällsviktiga tjänster rörande hälso- och sjukvård där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses;

- hälso- och sjukvård som bedrivs av en vårdgivare och som omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125) eller detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel,
- där antalet anställd legitimerad vårdpersonal eller på annat sätt anlitad legitimerad vårdpersonal överstiger 50 årsarbetskrafter, eller
- där minst 20 000 expedieringar av receptbelagda läkemedel utförs per år.

Socialstyrelsens förslag till föreskrifter innehåller bland annat krav på vad en riskanalys ska innehålla, grundläggande tekniska och organisatoriska åtgärder samt grundläggande åtgärder för att upprätthålla kontinuitet i den samhällsviktiga tjänsten. Tillsammans med MSB:s förskrifter om hur ett systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas, kommer de föreslagna föreskrifterna att utgöra en tydlig reglering som anger hur kraven på säkerhetsåtgärder enligt NIS-lagen ska uppfyllas.

Förslaget

Föreskriftsförslaget anger hur NIS-lagen ska tillämpas och gäller för leverantörer som avses i NIS-lagen och som tillhandahåller samhällsviktiga tjänster inom sektorn hälso- och sjukvård.

Av föreskriftsförslaget framgår bland annat;

- att leverantören ska analysera sina nätverk och informationssystem för att identifiera vilka nätverk och informationssystem som används

- vad den riskanalys och åtgärdsplan som leverantören ska upprätta enligt NIS-lagen ska innehålla
- vad leverantören ska beakta vid framtagandet av riskanalysen
- vad leverantören ska dokumentera i samband med riskanalysarbetet
- vilka säkerhetsåtgärder som leverantören ska vidta om riskanalysen påvisar ett sådant behov
- att leverantören ska vidta de ytterligare åtgärder som är nödvändiga för att hantera de risker som framkommit i riskbedömningen

Kostnadsmässiga och andra konsekvenser

Förslaget till föreskrifter innehåller krav rörande de organisatoriska och tekniska säkerhetsåtgärder som leverantörer av samhällsviktiga tjänster inom hälso- och sjukvårdssektorn är skyldiga att vidta enligt NIS-lagen. Eftersom NIS-lagen trädde i kraft 2018 bör samtliga leverantörer som berörs av de föreslagna föreskrifterna redan arbeta med riskanalyser och åtgärdsplaner. De grundläggande kraven framgår redan av lag. De kostnadsmässiga konsekvenser som skulle kunna uppstå till följd av det presenterade förslaget till nya föreskrifter bör därför enligt utredningen främst bestå av mindre administrativa engångskostnader för de verksamheter som behöver anpassa sina nuvarande processer och rutiner så att de överensstämmer med de föreslagna kraven.

Hur verksamheter arbetar med riskanalyser och åtgärdsplaner skiljer sig också mycket leverantörerna emellan. Vissa riskanalyser genomförs på enhetsnivå medan andra genomförs på central nivå. Det finns också stora variationer i antalet nätverk och informationssystem per leverantör eftersom leverantörerna gör sina egna bedömningar om vad som bör klassificeras som ett nätverk och informationssystem. De stora variationerna i leverantörernas arbete med informationssäkerhet idag gör att det inte har varit möjligt för Socialstyrelsen att uppskatta de totala kostnadsmässiga konsekvenserna av de förslagna föreskrifterna.

Remissammanställningen

Ärendet har remitterats till stadsledningskontoret, socialnämnden och äldrenämnden. Socialförvaltningen och äldreförvaltningen har inkommit med kontorsyttrande.

Stadsledningskontoret

Stadsledningskontorets tjänsteutlåtande daterat den 17 januari 2024 har i huvudsak följande lydelse.

Stadsledningskontoret ställer sig positiva till Socialstyrelsens förslag till föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn och ser att de kommer stödja stadens systematiska informationssäkerhetsarbete. I och med att NIS-lagstiftningen kom 2018 så arbetar staden redan med frågorna, vilket innebär att stadsledningskontoret gör bedömningen att inga omedelbara kostnader för

organisatoriska åtgärder kommer uppstå med koppling till föreskrifterna. Vad gäller kostnader för eventuella tekniska åtgärder är dessa i dagsläget svåra att bedöma.

Stadsledningskontoret ser behov av några kompletteringar och förtydliganden för att säkerställa syftet med föreskrifterna.

I syfte att säkerställa att termer används konsekvent mellan regelverk, kan en manual med termer och begrepp som förekommer i föreskriften underlätta tolkning och förståelse.

Stadsledningskontoret välkomnar vidare att föreskrifterna tydliggör kopplingen mellan nätverk och informationssystem för tillhandahållandet av samhällsviktig tjänst och säkerställande av kontinuitet.

För att säkerställa en systematik som inkluderar ständiga förbättringar föreslås en komplettering med utvärdering av vald metod för riskanalysmetod i 7 §. Vidare kan krav på åtgärdsplan i 9 § kompletteras med modell och nivåer för riskacceptans för att ytterligare tydliggöra och motivera valda åtgärder för identifierade risker. Utan modell för riskacceptans blir motivering av vidare hantering av risker otydlig.

I 10 § anger föreskriften att samtliga tekniska lösningar ska beaktas vid bedömning av vilka säkerhetsåtgärder som ska vidtas. Stadsledningskontoret föreslår att ”samtliga” ersätts av ”lämpliga” för att föreskriftens reglering dels ska vara i linje med Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, dels vara möjliga att efterleva i praktiken.

Vidare föreslår stadsledningskontoret ett förtydligande av innebörden av ”systemadministratör” i 13 §. Detta för att förtydliga en skillnad mellan en användare som har höga behörigheter för att utföra uppgifter i systemet från den administratör som utför uppgifter med själva systemet såsom underhåll, databasadministration, och uppgradering.

Den inledande meningen i 18 § kan med fördel skrivas om för att öka läsbarheten och det avslutande stycket förenklas genom en omformulering liknande ”Användare ska framgå om…”

Stadsledningskontoret föreslår att avsnittet om incidenthantering kompletteras med krav på återföring av erfarenheter från incidenter till riskanalysarbetet för att säkerställa förbättringar och lärande utifrån inträffande händelser.

Stadsledningskontoret föreslår att kommunstyrelsen beslutar att Socialstyrelsens remiss Förslag till föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn besvaras med hänvisning till vad som sägs i stadsledningskontorets tjänsteutlåtande.

Socialförvaltningen

Socialförvaltningens tjänsteutlåtande daterat den 8 januari 2024 har i huvudsak följande lydelse.

Socialförvaltningen ställer sig positiva till Socialstyrelsens förslag till föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvårdssektorn och ser att de kommer stödja förvaltningens systematiska informationssäkerhetsarbete. Då NIS-lagstiftningen kom 2018, så arbetar förvaltningen med frågorna vilket innebär att förvaltningen gör bedömningen att inga omedelbara kostnader för organisatoriska åtgärder kommer uppstå med koppling till föreskrifterna. Vad gäller kostnader för eventuella tekniska åtgärder är dessa i dagsläget svåra att bedöma. Dock vill förvaltningen lyfta att informationssäkerhetsarbete generellt är ett prioriterat och omfattande område, vilket kan komma att medföra ökade kostnader på sikt för hela Stockholms stad oavsett dessa föreslagna föreskrifter.

Förvaltningen ser behov av förtydligande för att säkerställa syftet med föreskrifterna.

I syfte att säkerställa att termer används konsekvent mellan regelverk, kan en manual med termer och begrepp som förekommer i föreskriften underlätta tolkning och förståelse. Förvaltningen välkomnar vidare att föreskrifterna tydliggör kopplingen mellan nätverk och informationssystem för tillhandahållandet av samhällsviktig tjänst och säkerställande av kontinuitet.

För att säkerställa en systematik som inkluderar ständiga förbättringar föreslås en komplettering med utvärdering av vald metod för riskanalysmetod i 7 §. Vidare kan krav på åtgärdsplan i 9 § kompletteras med modell och nivåer för riskacceptans för att ytterligare tydliggöra och motivera valda åtgärder för identifierade risker. Utan modell för riskacceptans blir motivering av vidare hantering av risker otydlig.

I 10 § anger föreskriften att samtliga tekniska lösningar ska beaktas vid bedömning av vilka säkerhetsåtgärder som ska vidtas. Förvaltningen föreslår att ”samtliga” ersätts av ”lämpliga” för att föreskriftens reglering dels ska vara i linje med Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, dels vara möjliga att efterleva i praktiken.

Vidare föreslår förvaltningen ett förtydligande av innebörden i ”systemadministratör” i 13 §. Detta för att förtydliga en skillnad mellan en användare som har höga behörigheter för att utföra uppgifter i systemet från den administratör som utför uppgifter med själva systemet såsom underhåll, databasadministration, och uppgradering.

Den inledande meningen i 18 § kan skrivas om för att öka läsbarheten och det avslutande stycket förenklas genom en omformulering liknande ”Användare ska framgå om…”

Förvaltningen föreslår att avsnittet om incidenthantering kompletteras med krav på återföring av erfarenheter från incidenter till riskanalysarbetet för att säkerställa förbättringar och lärande utifrån inträffande händelser.

Socialförvaltningens kontorsutlåtande översänds till kommunstyrelsen som svar på remissen.

Äldreförvaltningen

Äldreförvaltningens tjänsteutlåtande daterat den 11 januari 2024 har i huvudsak följande lydelse.

Förvaltningen har beretts möjlighet att lämna synpunkter på förslaget till föreskrifter om säkerhetsåtgärder för samhällsviktiga tjänster inom hälso- och sjukvården. Förvaltningen har inget att invända mot förslaget. Förvaltningen ser positivt på föreskrifterna och att de kommer ge stöd i utformningen av det systematiska informationssäkerhetsarbetet. Förvaltningen gör bedömningen att förslaget inte medför några kostnader eller annan negativ påverkan på verksamheten.

Förvaltningen föreslår följande förtydliganden för att säkerställa syftet med föreskrifterna.

För att säkerställa att termer används konsekvent mellan regelverk kan en lista med termer och begrepp som förekommer i föreskriften underlätta tolkning och förståelse.

Förvaltningen välkomnar att föreskrifterna tydliggör kopplingen mellan nätverk och informationssystem för tillhandahållandet av samhällsviktig tjänst och säkerställande av kontinuitet.

För att säkerställa en systematik som inkluderar ständiga förbättringar föreslår vi en komplettering med utvärdering av vald metod för riskanalysmetod i 7 §. Vidare kan krav på åtgärdsplan i 9 § kompletteras med modell och nivåer för riskacceptans för att ytterligare tydliggöra och motivera valda åtgärder för identifierade risker. Utan modell för riskacceptans blir motivering av vidare hantering av risker otydlig.

I 10 § anger föreskriften att samtliga tekniska lösningar ska beaktas vid bedömning av vilka säkerhetsåtgärder som ska vidtas. Förvaltningen föreslår att ”samtliga” ersätts av ”lämpliga” för att föreskriftens reglering dels ska vara i linje med Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, dels vara möjliga att efterleva i praktiken.

Vidare föreslår förvaltningen ett förtydligande av innebörden i ”systemadministratör” i 13 §. Detta för att förtydliga en skillnad mellan en användare som har höga behörigheter för att utföra uppgifter i systemet från den administratör som utför uppgifter med själva systemet såsom underhåll, databasadministration, och uppgradering

Den inledande meningen i 18 § kan skrivas om för att öka läsbarheten och det avslutande stycket förenklas genom en omformulering liknande ”Användare ska framgå om…”

Förvaltningen föreslår att avsnittet om incidenthantering kompletteras med krav på återföring av erfarenheter från incidenter till riskanalysarbetet för att säkerställa förbättringar och lärande utifrån inträffande händelser.

Förvaltningen förslår att äldrenämnden godkänner förvaltningens tjänsteutlåtande som svar på remissen och överlämnar det till kommunstyrelsen.