Gävle KOMMUN

Yttrande

Dnr 24KS149-5
2024-05-20

Kommunstyrelsen

Adrian Henriksson Severin
Telefon 026-17 80 64
adrian.henriksson_severin@gavle.se

Yttrande över delbetänkande 2024:18 Nya regler om cybersäkerhet

Ert diarienummer: Fö2024/00496

Beskrivning av ärendet

Regeringen beslutade den 23 februari 2023 att tillkalla en särskild utredare med uppgift att föreslå de anpassningar av svensk rätt som är nödvändiga för att EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) ska kunna genomföras. Den 5 mars 2024 publicerades delbetänkandet ”Nya regler om cybersäkerhet” (SOU 2024:18). Gävle kommun har blivit ombedd att yttra sig över betänkandet.

Yttrande

Gävle kommun tillstryker till del utredningens förslag om hur Europaparlamentets och rådets direktiv av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) ska implementeras i Sverige.

Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs. Gävle kommun är i huvudsak positiva till förslaget men konstaterar samtidigt att vissa ändringar bör göras. Förslag kommer i vissa fall att innebära dubbelarbete och ett ineffektivt nyttjande av såväl kommunens som statens resurser.

Gävle kommun följande synpunkter:

En väg in för verksamhetsutövarens anmälan

Utredningen föreslår att en verksamhetsutövares anmälan om att den omfattas av NIS2-regleringen ska göras till respektive tillsynsmyndighet (se 2 kap. 2§ i förslag till cybersäkerhetslagen). Enligt utredningen är respektive kommun en verksamhetsutövare. I regel bedriver en kommun verksamhet inom flera av de sektorer som föreslås omfattas av cybersäkerhetslagen som i sin tur innebär att kommunen som verksamhetsutövare berörs av flera tillsynsmyndigheter. För Gävle kommun kommer det, utifrån utredningens förslag, åtminstone handla om två tillsynsmyndigheter.

Gävle kommun menar att tillvägagångssättet inte är rimligt eller resurseffektivt. Dessutom, beroende på hur många tillsynsmyndigheter det handlar, finns risken för att vissa uppgifter kan missas att ändras när så krävs. Lägg där till att respektive tillsynsmyndighet inom sitt tillsynsområde ska upprätta ett register över väsentliga och viktiga verksamhetsutövare samt ha en tillräckligt säker hantering av detta register. Inriktningen torde vara att de organisationer som omfattas av NIS2-regleringen ska ha lätt att göra sin plikt.

Genom att tillhandahålla en väg in för verksamhetsutövarens anmälan skulle verksamhetsutövaren endast behöva göra en anmälan som sedan distribueras till den eller de tillsynsmyndigheter som berörs. Förslagsvis kan en sådan anmälan lämnas till Myndigheten för samhällsskydd och beredskap (MSB).

Ge en myndighet i uppgift att föreskriva om riskhanteringsåtgärder, med mera alternativt stärk samordningen av tillsynsmyndigheternas föreskrifter

Utredningen föreslår att lagen bör fyllas ut av föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning som meddelas av tillsynsmyndigheterna. Myndigheten för samhällsskydd och beredskap, MSB, ska ges tillfälle att yttra sig över föreskrifterna och regeringen föreslås ge MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete. Enligt utredningens uppfattning är det angeläget att föreskrifterna kan anpassas sektorsvis och att den myndighet som har tillsyn också har föreskriftsrätt.

Som beskrivits tidigare bedriver en kommun verksamhet inom flera av de sektorer som föreslås omfattas av cybersäkerhetslagen som i sin tur innebär att kommunen som verksamhetsutövare berörs av flera tillsynsmyndigheter. I det här fallet innebär det att kommuner kommer behöva förhålla sig till flera olika föreskrifter som alla behandlar krav på riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning.

Gävle kommuns bedömning är att utredningens förslag riskerar att leda till fragmentering av området, ett flertal överlappande föreskrifter med onödiga kostnader och ett resursineffektivt arbete som konsekvens. Med anledning av detta instämmer Gävle kommun med det förslag som flera expertmyndigheter lämnade i utredning, att MSB ska ges befogenhet att meddela grundföreskrifter för samtliga sektorer. Tillsynsmyndigheterna kan sedan, vid behov och med stöd av sin sektorsspecifika kompetens, komplettera grundföreskrifterna med särskilda föreskrifter med stärkta krav där behoven inom sektorn kräver det. I annat fall ser Gävle kommun att samordningen av tillsynsmyndigheternas föreskrifter stärks. Endast ett yttrande från MSB är inte tillräckligt.

Stärk tillsynssamordningen

Av 13§ i förslaget till cybersäkerhetsförordningen framgår att *”Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive*

tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §."

Gävle kommun är positiv till 13§ men ser samtidigt en utmaning i den praktiska tillämpningen av den. Enligt kommunens bedömning innebär det att delar av verksamhetens nätverk och informationssystem kan komma att bli tillsynade av flera berörda tillsynsmyndigheter. Exempelvis kan ett informationssystem användas i flera verksamhetsområden (sektorer) hos en och samma verksamhetsutövare. Så är fallet för hälso- och sjukvård och socialtjänst där många kommuner använder ett och samma informationssystem. I sådana system har respektive verksamhetsområde har sin modul. Detta kan bli kostnadsdrivande samt medföra en risk för oförenliga krav och sanktioner. För en kommun kan det även gälla nätarkitektur, IT-drift, användning av kommunövergripande applikationer och program: Sammantaget kan det vid en tillsyn vara svårt att peka ut de olika ansvarsområdena.

Utredning menar att det får förutsättas att tillsynsmyndigheterna samarbetar vid genomförande av tillsyn rörande verksamhetsutövare som bedriver verksamhet i flera sektorer. Det följer av förvaltningslagen och myndighetsförordningen och behöver inte anges särskilt i regleringen menar utredningen. Det som anförs i utredningen bygger på att tillsynsmyndigheterna har vetskap om att en viss verksamhetsutövare bedriver verksamhet i flera sektorer. Gävle kommun anser därför att tillsynssamordning bör regleras ännu starkare i cybersäkerhetsförordningen, särskilt i de fall en verksamhetsutövare bedriver verksamhet i flera sektorer.

Respektive nämnd i en kommun borde utgöra en verksamhetsutövare

Gävle kommun ser positivt på att kommunerna föreslås omfattas av cybersäkerhetslagen samt att kommuner anses vara väsentliga. Däremot delar inte kommunen utredningens uppfattning att kommuner ska anses vara en och samma verksamhetsutövare. Respektive nämnd i en kommun borde utgöra en verksamhetsutövare likt statliga myndigheter.

Sveriges kommun och regioner, SKR, har i utredningen anfört att det inte nödvändigt att det är kommunen som juridisk person som är verksamhetsutövare och att kommunen därmed utgör en enhet. SKR menar att det skulle vara möjligt att se en nämnd inom kommunen, som inte är en egen juridisk person, som en särskild enhet. Utredningen delar inte SKR:s uppfattning och menar i stället att nämnder, till skillnad från statliga myndigheter, inte får företräda kommunen i domstol eller föra talan i frågan om exempelvis sanktionsavgifter. Utredningen hänvisar till 6 kap. 15 § kommunallagen (2017:725) som säger att styrelsen får själv eller genom ombud företräda kommunen eller regionen i alla mål och ärenden, om inte någon annan ska göra det på grund av lag eller annan författning eller beslut av fullmäktige. Detta synsätt är närmst förvirrande och har inte med saken att göra. Vad som i stället behöver uppmärksammas är att varje nämnd är en egen förvaltningsmyndighet och självständigt i förhållande till andra sådana myndigheter; exempelvis i fråga om tillämpning av lag (Jfr. 12 kap. 2 §

regeringsformen). Kommunfullmäktige kan besluta att kommunstyrelsen får besluta om andra nämnders verksamhet men inte i fråga om tillämpning av lag. Den avgörande frågan är hur den interkommunala kompetensfördelningen ska se ut; exempelvis en kommunstyrelsens mandat att meddela föreskrifter till nämnderna hur de ska fullgöra uppgifter i den nya lagen.

I tillämpning av närliggande reglering, exempelvis av den allmänna dataskyddsförordningen[1], är respektive nämnd i en kommun personuppgiftsansvarig. I dataskyddsförordningen, likt i den föreslagna cybersäkerhetslagen, finns möjligheter för tillsynsmyndigheten att lämna sanktioner mot personuppgiftsansvarig. Integritetsskyddsmyndigheten, IMY, har meddelat flera sanktionsbeslut mot nämnder hos både regioner och kommuner.[2] Gävle kommun finner därför att de skäl som utredningen framhåller inte är relevanta. Med anledning av det som anförts anser kommunen att respektive nämnd ska utgöra en verksamhetsutövare.

I avsnitt 5.2.10 redogör utredningen för sitt resonemang och lyfter bland annat fram att majoriteten av alla kommuner, omfattas av NIS2-direktivets krav redan genom att en stor andel av samtliga kommuner bedriver hemsjukvård och att samtliga uppfyller storlekskravet. Vidare lyfter utredningen att det är kommunen som juridisk person som omfattas som vårdgivare. Vidare menar utredningen att det därmed saknas skäl att överväga om kommuner ska ses som offentliga förvaltningsverksamheter på lokal nivå enligt artikel 2.5 a. Utredningen föreslår dock i fullständighetens namn att alla kommuner omfattas, men att kommunfullmäktige undantas. Gävle kommun menar att det är olyckligt, utredningen borde tagit tillfället i akt att utreda huruvida kommuner ska ses som offentliga förvaltningsverksamheter på lokal nivå. Särskilt eftersom Gävle kommun menar att respektive nämnd bör vara verksamhetsutövare.

Tydliggör om och på vilket sätt kommunalförbund omfattas av den förslagna cybersäkerhetslagen

Som nämnt ovan är Gävle kommun positiva till att kommunerna föreslås omfattas av den föreslagna lagen. Kommunallagen (2017:725) ger kommunerna möjlighet att bilda kommunalförbund och lämna över skötseln av kommunala angelägenheter till sådana förbund (3 kap. 8§ kommunallagen). Flera kommuner är medlemmar i kommunalförbund och de förbund som finns har skötsel av vitt skilda kommunala angelägenheter. Gävle kommun är exempelvis med i ett räddningstjänstförbund och ett förbund som bedriver avfallshantering. Gävle kommun vill framhålla att det är en brist i att utredningen inte berör om och på vilket sätt kommunalförbund eventuellt omfattas av den föreslagna cybersäkerhetslagen.

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.
[2] Se exempelvis IMYs beslut DI-2019-2221, DI-2019-7321, DI-2021-5595 och IMY-2023-1647.

Gävle kommuns uppfattning är att det är kommunen som organisation som föreslås omfattas. Detta med anledning av att kommunerna bedriver hemsjukvård. Som redogjordes för ovan har utredningen inte tagit övervägt om kommuner ska ses som offentliga förvaltningsverksamheter på lokal nivå enligt artikel 2.5 a. Detta kan få effekten att verksamhet i en kommun kan omfattas av kraven i den föreslagna lagen medan verksamhet i en annan kommun inte omfattas då den är förlagd hos ett kommunalförbund. Vissa kommuner har räddningstjänsten i sin förvaltning medan andra har den i förbund. Vissa kommuner har lagt delar av sin socialtjänst eller motsvarande IT-avledningen i kommunalförbund. I några fall bedriver förbund verksamhet som hör till någon av de sektorer som föreslås omfattas av cybersäkerhetslagen. Så är fallet för förbund inom sektorn avfallshantering.

Kommunens bedömning är att kommunalförbund inte går att likställa med kommuner i förslaget till cybersäkerhetslagen. Det innebär att de förbund som bedriver sådan verksamhet som annars bedrivits av kommunerna inte kommer omfattas av lagen till följd av att organiserat i ett kommunalförbund. Krasst uttryckt kan kommunerna lägga verksamhet i kommunalförbund för att på så sätt komma förbi cybersäkerhetslagen under förutsättning att verksamheten i fråga inte omfattas av någon av de sektorer som omfattas av lagen. Gävle kommen tycker att det behöver tydliggöras om och på vilket sätt kommunalförbund föreslås omfattas av lagen, likt hur utredningen berör kommunala bolag.

Använd etablerade begrepp

Som anförs i avsnitt 5.2.1 är utredningens utgångspunkt att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt. Ett normalt språkbruk ska eftersträvas. Utredningen menar att det uttryckligen följer regeringens direktiv att den terminologi som används i direktiven ska anpassas till vedertagna begrepp i nationell reglering.

Gävle kommun instämmer i att vedertagna begrepp och ett normalt språkbruk ska användas. Kommunen anser därför att begreppet ”riskhanteringsåtgärder” ska ersättas med ”säkerhetsåtgärder” för att uppfylla såväl utredningens utgångspunkt som regeringens direktiv att den terminologi som används i direktiven ska anpassas till vedertagna begrepp i nationell reglering.

Utredningens bedömning att kraven i NIS2-direktivet i hög grad skiljer sig från kraven i NIS-direktivet håller inte Gävle kommun med om. Skillnaden mellan direktiven är snarare att kraven konkretiseras i NIS2-direktivet i jämförelse nuvarande NIS-reglering. Vidare utgör inte utrednings bedömning ett skäl till att etablera nya begrep. Gävle kommun anser därför att ”säkerhetsåtgärder” är det etablerade begreppet som ska användas. Det är angeläget att cybersäkerhetsregelverket så långt som möjligt ansluter sig till vedertagen begreppsanvändning eftersom verksamhetsutövarna redan är väl bekanta med dem. Dessutom används ”säkerhetsåtgärder” som begrepp i annan närliggande reglering som exempelvis dataskyddsförordningen, patientdatalag (2008:355) och patientdataförordning (2008:360).

Säkerhetsåtgärder är ett etablerat samlingsbegrepp för åtgärder som kan införas för att skydda nätverk och informationssystem, både nationellt och internationellt. Att byta begreppet ”säkerhetsåtgärder” mot ”riskhanteringsåtgärder” riskerar att skapa en felaktig bild av att det är något annat än den etablerade uppsättningen av åtgärder som används för att skydda nätverk och informationssystem.

Utredningen menar att det skulle bli förvirrande att använda samma begrepp när kraven i hög grad är nya. Kommunen menar å andra sidan att det blir förvirrande att använda olika begrepp för samma typ av åtgärd utifrån olika regleringar. Ponera att en verksamhet vidtar en åtgärd i systemet X. Utifrån dataskyddsförordningen skulle åtgärden anses vara en säkerhetsåtgärd men utifrån cybersäkerhetslagen skulle samma åtgärd anses vara en riskhanteringsåtgärd. Detta skulle bli förvirrande för verksamhetsutövarna.

Gävle kommun ser också att formuleringen ”systematiskt och riskbaserat informationssäkerhetsarbete” kompletteras med ”cybersäkerhet” med anledning av att EU har definierat cybersäkerhet i cybersäkerhetsakten och att begreppet genomgående används i övriga delar av betänkandet. Den röda tråden i betänkandet samt lagförslaget blir tydligare och eventuella diskussioner som skiljelinjen mellan systematiskt och riskbaserat informationssäkerhetsarbete å ena sidan och cybersäkerhet å andra sidan kan undvikas. Ett systematiskt och riskbaserat informations- och cybersäkerhetarbete är heltäckande och tydliggör ett allriskperspektiv i arbetet med skydd för nätverk och informationssystem.

Beslutsunderlag

Delbetänkande - Nya regler om cybersäkerhet (SOU 2024:18)

Remiss - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18).

Adrian Henriksson Severin
Infosäkerhetssamordnare
Administrativa avdelningen