AVFALL SVERIGE

PM nr. 7 2025

Reviderat cybersäkerhetsdirektiv (NIS2)

Maj 2025

Avfall Sverige, Avfall Sverige AB, Baltzarsgatan 25, 211 36 Malmö, Telefon 040-35 66 00
E-post info@avfallsverige.se, Hemsida www.avfallsverige.se, Bankgiro 985-9877, Organisationsnummer 556260-8553

Sammanfattning

- NIS2-direktivet[1] är en revidering av EU:s första cybersäkerhetsdirektiv[2]. NIS2-direktivet syftar till att stärka cybersäkerheten inom EU och ställer krav på att företag ska arbeta systematiskt och riskbaserat med informationssäkerhet. NIS2-direktivet omfattar verksamheter inom ett stort antal sektorer, vilka delas in kategorierna ”viktiga” och ”väsentliga”.

- Utöver att NIS2-direktivet omfattar fler sektorer än det första cybersäkerhetsdirektivet har det tillkommit andra viktiga förändringar. Bland annat föreskrivs ett ledningsansvar, vilket innebär att ledningen (i regel styrelsen och dess suppleanter samt vd) har ansvar för att godkänna, och övervaka genomförandet av, de säkerhetsåtgärder som införs för att efterleva NIS2-direktivet, och att ledningen kan ställas till svars för eventuella överträdelser av dem. Genom NIS2-direktivet införs även förstärkta incidentrapporteringskrav, det läggs större vikt vid cybersäkerhet i företagens leveranskedja och dessutom har påföljderna vid överträdelser av NIS2-direktivet skärpts.

- Eftersom NIS2-direktivet är ett direktiv behöver det införlivas i svensk rätt. Den svenska kompletterande lagstiftningen skulle ha antagits av Sverige senast den 17 oktober 2024 och börjat tillämpas senast den 18 oktober 2024. Detta har dock inte skett vid tidpunkten för upprättandet av detta dokument. I och med detta har som rättskällor endast kunnat användas av direktivtexten och SOU 2024:18 Nya regler om cybersäkerhet (”SOU:n”, ”utredningen”).

- Utredningen som föregått, och summeras i, detta dokument är därmed gjord med förbehåll för att den kan komma att påverkas av eventuella ändringar och/eller ändrade förutsättningar i propositionen, publicerad lag och förordning samt kompletterande myndighetsföreskrifter.

[1] Europaparlamentets och Rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (NIS2).
[2] Europaparlamentets och Rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS).

1. På vilket sätt omfattas Avfall Sveriges kommunmedlemmar av bestämmelserna i NIS2-direktivet?

1.1 Introduktion

För att avgöra om Avfall Sveriges kommunmedlemmar omfattas av NIS2-direktivet behöver det till en början avgöras om artikel 2.1 i NIS2-direktivet är tillämplig på kommunmedlemmarnas verksamhet. Enligt artikel 2.1 omfattas offentliga och privata entiteter (verksamheter) av NIS2- direktivet under förutsättning att vissa kriterier är uppfyllda. Bland annat ska verksamheten bedrivas inom någon av de sektorer som framgår av NIS2-direktivets bilaga I och II (det så kallade ”sektorkriteriet”), vidare ska verksamheten sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro på koncernnivå (det så kallade ”storlekskriteriet”).

I och med ovan måste det alltså först utredas om kommunmedlemmarnas verksamheter faller inom någon av de sektorer som stadgas i bilaga I och II till NIS2-direktivet.

1.2 Offentlig förvaltning

Offentlig förvaltning är en egen utpekad sektor i NIS2-direktivet. I bilaga I beskrivs sektorn som (i) offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt, samt (ii) offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt. Det finns även en särskild definition av offentlig förvaltningsentitet i artikel 6 punkt 35 i direktivet, där följande fyra kriterier ska uppfyllas för att en entitet ska falla in under definitionen:

(i) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

(ii) Den har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person.

(iii) Den finansieras till största delen av staten, regionala myndigheter eller andra offentligrättsliga organ, står under administrativ tillsyn av dessa myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ.

(iv) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

Genom artikel 2.2 f i NIS2-direktivet stadgas i tillägg till ovan att de offentliga förvaltningsentiteter som framgår av bilaga I och II inte behöver uppfylla storlekskriteriet för att omfattas av NIS2- direktivet, utan de omfattas som utgångspunkt oavsett storlek.

I Sverige bedrivs den offentliga förvaltningen genom statliga och kommunala förvaltningsorgan och begreppet förvaltningsmyndighet omfattar alla myndigheter utom regeringen och domstolarna. I NIS2-direktivets definition av offentlig förvaltning omfattas dock (enligt ovan) endast förvaltningsentiteter på nationell nivå, så som statliga myndigheter, och regional nivå, så som de regionala nämnderna. Kommuner omfattas till följd därav inte utav sektorn ”offentlig förvaltning” såsom den definieras i NIS2-direktivet. Avfall Sveriges kommunmedlemmar omfattas därmed inte av NIS2-direktivet enligt nämnda beskrivning i bilaga I.

I SOU:n resoneras till följd av ovan kring vad som gäller för kommuner och kommunala bolag och det görs en distinktion mellan dessa. I det följande utreds vad som gäller för kommuner, därefter för kommunalförbund och till sist kommunala bolag.

1.3 Kommuner

Även om kommuner inte omfattas av sektorn offentlig förvaltning i bilaga I konstateras i SOU:n att kommunerna (i) uppfyller de fyra kriterierna som ställs på offentliga förvaltningsentiteter (se ovan), samt (ii) bedriver sådan verksamhet som utgör utpekade sektorer/områden i bilaga I och II. Exempel på sådan verksamhet är fjärrvärme, hemsjukvård och avfallshantering (även om det i utredningen påtalas att avfallshantering i många fall bedrivs genom kommunala bolag). I utredningen konstateras därefter att enligt uppgifter från SKR uppfyller alla kommuner i vart fall storlekskriteriet.

Baserat på ovan dras slutsatsen att de flesta kommuner, i sin helhet, genom att bedriva hemsjukvård, kommer att omfattas av NIS2-direktivet. Utredningen föreslår därmed att alla kommuner omfattas, även de som inte bedriver hemsjukvård. I det av utredningen framlagda förslag till lag om cybersäkerhet (dvs. den lag som implementerar NIS2-direktivet) framgår därmed i dess 3 § att kommuner (i) faller in under definitionen ”offentliga verksamhetsutövare”, och (ii) omfattas av lagen i dess helhet[3]. Avfall Sveriges medlemmar i form av kommuner omfattas därmed av NIS2-direktivet såsom det för närvarande har för avsikt att implementeras i svensk rätt.

1.4 Kommunalförbund

Kommunalförbund nämns inte i SOU:n. Mot bakgrund av det resonemang som förs avseende kommuner i SOU:n är vår bedömning att kommunalförbund bör – förutsatt att dessa uppfyller de krav som ställs på offentlig förvaltningsentitet i artikel 6 punkt 35 i NIS2-direktivet samt att de bedriver verksamhet inom någon av de sektorer som utpekas i bilaga

[3] Med undantag för kommunfullmäktige.

I och II till NIS2-direktivet – i likhet med kommunerna, omfattas av NIS2-direktivet såsom det för närvarande har för avsikt att implementeras i svensk rätt.

1.5 Kommunala bolag

Som påtalats ovan (se avsnitt 2.3) beskrivs i SOU:n att avfallshantering i många fall bedrivs genom kommunala bolag. Enligt utredningens bedömning är det i den situationen inte kommunen som är verksamhetsutövare utan det kommunala bolaget. Utredningen gör denna bedömning bland annat med hänvisning till att kommunala bolag, som vanligen bedrivs i form av aktie- eller handelsbolag, inte kan rikta administrativa eller andra beslut mot fysiska eller juridiska personer (fjärde kriteriet som nämns ovan, se 2.2(iv)).

Därmed faller kommunala bolag utanför begreppet ”offentliga verksamhetsutövare” och till följd därav behöver det, i varje enskilt fall, göras en bedömning av huruvida verksamheten uppfyller sektorkriteriet respektive storlekskriteriet (se avsnitt 2.1). I de fall de kommunala bolagen uppfyller sektorkriteriet (avfallshantering) samt storlekskriteriet omfattas deras verksamhet av NIS2-direktivet.

Avslutningsvis bör tilläggas att sektorn avfallshantering i bilaga II beskrivs som verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG, dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är avfallshantering. Av definitionen i direktiv 2008/98/EG framgår att med avfallshantering menas ”insamling, transport, återvinning och bortskaffande av avfall, inklusive kontroll av sådan verksamhet och efterbehandling av platser för bortskaffande av avfall, inklusive åtgärder som handlaren eller mäklaren vidtar”. Det finns i nuläget inte någon ytterligare information om vad som menas med avfallshantering enligt direktivets mening, och var gränsdragningen går i förhållande till ”verksamhetsutövare vars huvudsakliga näringsverksamhet inte är avfallshantering”. Eftersom det i utredningen inte utvecklas hur det ses på detta undantag, och att det i stället ges som exempel att kommuner och kommunala bolag bedriver just avfallshanteringsverksamhet bör det, enligt vår bedömning, i nuläget inte göras en extensiv tolkning av undantaget. De kommunala bolagen som bedriver avfallshantering bör därmed falla in under bestämmelserna i NIS2-direktivet, givet att storlekskriteriet är uppfyllt.

2. Åtgärder som behöver vidtas

2.1 Introduktion

Enligt redogörelse i tidigare avsnitt omfattas sannolikt Avfall Sveriges kommun-, kommunalförbunds- samt kommunala bolagsmedlemmar av NIS2-direktivet. Följande avsnitt beskriver de åtgärder som varje verksamhet/medlem bör vidta för att uppfylla kraven i direktivet. Det bör nämnas att de svenska tillsynsmyndigheterna, i tillägg till

nedan, kommer att meddela närmare föreskrifter anpassade till respektive sektor, där exempelvis riskhanteringsåtgärder kommer att specificeras.

2.2 Allokera resurser och utse styrgrupp

NIS2-direktivet ställer ett flertal olika krav på de verksamheter som omfattas av direktivet. Det är därför viktigt att, på ett tidigt stadium, allokera resurser för att utreda vilka krav som är relevanta för verksamheten och vilka brister som finns i nuvarande verksamhet. Vidare bör där utses en styrgrupp där rätt personer och funktioner involveras. Vilka funktioner som bör involveras är olika för olika verksamheter, dock bör t.ex. IT-kompetens och juridisk kompetens finnas inom styrgruppen. Inom styrgruppen bör även tydliga ansvarsområden allokeras och en plan för framtiden sättas upp. Det ska arbetas systematiskt och riskbaserat med informationssäkerhet över tid.

2.3 Utbildning

Det finns ett uttryckligt och lagstadgat krav på att ledningsgrupper inom enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder (se nedan under punkten 3.5). I tillägg till detta ska även verksamhetens resterande anställda erbjudas sådan utbildning.

Vad gäller ledningsgrupper bör särskilt noteras att NIS2-direktivet föreskriver ett ledningsansvar. Detta innebär, förutom kravet på utbildning, att ledningen ska godkänna de riskhanteringsåtgärder som vidtas, övervaka dess implementering och kan hållas ansvarig för överträdelser.

2.4 Anmälan av verksamhet till tillsynsmyndighet

När den svenska cybersäkerhetslagen träder i kraft ska verksamhetsutövare anmäla verksamheten till relevant tillsynsmyndighet. I utredningens förslag till förordning om cybersäkerhet föreslås Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län vara tillsynsmyndigheter för både avfallshantering och offentlig förvaltning.

Enligt förslaget till lag om cybersäkerhet ska anmälan till tillsynsmyndigheten innehålla uppgift om verksamhetsutövarens identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgifter om vilka länder verksamheten bedrivs. Det ska också anmälas om ändring görs av någon av uppgifterna.

3. Riskhanteringsåtgärder

Alla verksamheter behöver som nämnt vidta lämpliga och proportionella riskhanteringsåtgärder. Dessa ska vara verksamhetsanpassade och utgå ifrån ett allriskperspektiv. I det svenska förslaget till lag om cybersäkerhet listas följande områden inom vilka åtgärder ska vidtas:

- Incidenthantering (innebär bl.a. att en verksamhet ska etablera processer och rutiner för att identifiera, rapportera, hantera och återhämta sig från säkerhetsincidenter),
- kontinuitetshantering (innebär att planera och vidta förberedande åtgärder för att säkerställa att kritiska affärsfunktioner kan fortsätta under och efter en allvarlig incident eller kris),
- säkerhet i leveranskedjan (innebär att vidta åtgärder för att hantera risker som kan introduceras genom tredje part och verksamhetens egen leveranskedja),
- säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation (innebär bl.a. att vidta åtgärder för att säkerställa att säkerhetsaspekter beaktas vid inköp, utveckling och underhåll av IT-system och programvara),
- strategier och förfaranden för användning av kryptografi och kryptering (innebär bl.a. implementering av kryptografiska metoder för att skydda känslig information under lagring och överföring),
- personalsäkerhet (innebär bl.a. att vidta åtgärder för att säkerställa att verksamhetens personal inte utgör en säkerhetsrisk, inklusive att genomföra bakgrundskontroller),
- strategier för åtkomstkontroll och tillgångsförvaltning (innebär bl.a. implementering av system och processer för att kontrollera och begränsa tillgång till känslig information och systemresurser – inkl. tillgång till fysisk dokumentation),
- säkrade lösningar för kommunikation (innebär användning av säkra kommunikationskanaler för att skydda information som överförs elektroniskt), och
- lösningar för autentisering (innebär Implementering av system för att säkerställa att endast auktoriserade användare kan få tillgång till system och data, inklusive stark autentisering och multifaktorautentisering).

I SOU:n återfinns ingen detaljerad beskrivning av riskhanteringsåtgärderna då det framgår att utredningen vill ge utrymme för respektive tillsynsmyndighet att anpassa kraven till de olika sektorerna. Fram till dess att myndighetsföreskrifterna kommer på plats kan dock respektive verksamhet påbörja sitt arbete med utgångspunkt i existerande standarder – så som exempelvis ISO 27000-serien. Avfall Sverige rekommenderar även att policyarbetet påbörjas redan nu, exempelvis i förhållande till personalsäkerhet och incidenthantering.

Om promemorian

Underlag till promemorian har tagits fram av Setterwalls advokatbyrå i Malmö.
Kontakt på Avfall Sverige: Sven Lundgren sven.lundgren@avfallsverige.se,
tfn. 040-35 66 00.