Datum
2025-04-01

Er referens
Fi2026/00065

Tågföretagen

Finansdepartementet
fi.remissvar@regeringskansliet.se

Kopia
fi.ofa.dis.remisser@regeringskansliet.se.

Remissvar - Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115)

Tågföretagen är en bransch- och arbetsgivarorganisation med cirka 100 medlemmar som har närmare 19 000 medarbetare. Bland medlemmarna finns de flesta av Sveriges aktiva tågoperatörer och ett flertal järnvägsinfrastrukturföretag.

Tågföretagens bedömning – påverkan på järnvägsföretag

EU:s cyberresiliensförordning (Cyber Resilience Act) innebär att järnvägsföretag påverkas både direkt och indirekt genom skärpta och i vissa delar nya krav på cybersäkerhet för produkter och system som är centrala för järnvägens drift. Även om regelverket i första hand riktar sig till tillverkare och leverantörer av produkter med digitala element, får det i praktiken betydande konsekvenser för järnvägsföretag som användare och beställare av sådana system.

Digitala system och driftkritiska funktioner

Järnvägsföretag är i hög grad beroende av digitala produkter och system såsom signalsystem, trafikledning, kommunikationslösningar, fordons- och underhållssystem samt IT-stöd för operativ verksamhet. Dessa omfattas i stor utsträckning av cyberresiliensförordningens krav på bland annat risk- och sårbarhetshantering, dokumentation, säkerhetsuppdateringar samt rapportering av allvarliga incidenter och utnyttjade sårbarheter. Förordningen får därmed direkt betydelse för järnvägsföretagens möjligheter att bedriva säker och tillförlitlig verksamhet.

Ökat ansvar i leverantörs- och upphandlingsledet

Järnvägsföretag behöver i ökande utsträckning säkerställa att upphandlade produkter och tjänster uppfyller kraven enligt cyberresiliensförordningen. Detta innebär ett ökat ansvar i kravställning, uppföljning och kontroll av leverantörer, inklusive hantering av säkerhetsuppdateringar och incidenter under hela produktens livscykel. I vissa situationer kan järnvägsföretag även bedömas

omfattas av regleringen i egenskap av importör eller distributör, till exempel vid anpassning eller vidareanvändning av digitala produkter.

Järnvägssektorns fordonspark har typiskt en operativ livslängd om 30–40 år. En betydande andel av de system och fordon som är i trafik efter cyberresiliensförordningens tillämpningsdatum den 11 december 2027 har upphandlats under kontrakt ingångna långt innan förordningen trädde i kraft, och utan att cyberresilienskrav inkluderats i de tekniska specifikationerna. Rollfördelningen är därtill särskilt komplex vid upprustning och modifiering av befintliga fordon, eftersom ett järnvägsföretag – beroende på vem som genomför den sista integrationen av digitala komponenter – utan att ha avsett det kan träda in i tillverkarens rättsliga ställning med fullt ansvar för CRA-efterlevnad, teknisk dokumentation och CE-märkning avseende det sammansatta systemet.

Cyberresiliensförordningen är en EU-förordning med direkt tillämplighet, och dess begrepp – däribland *utsläppande på marknaden*, *väsentlig modifiering* och tillverkaransvarets fördelning vid delad systemintegration – är EU-rättsligt autonoma begrepp vars tolkning tillkommer kommissionen och ytterst EU-domstolen. Den nationella kompletterande lagstiftningen kan varken klargöra dessa begrepps innebörd eller reglera hur de ska tillämpas på pågående leveransavtal eller vid delad integration.

Tågföretagen uppmanar därför den svenska regeringen att på EU-nivå aktivt verka för att kommissionen utfärdar samlad vägledning om hur begreppen *utsläppande på marknaden*, *väsentlig modifiering* och tillverkaransvaret vid delad systemintegration ska tillämpas vid serieleveranser och upprustning av järnvägsfordon. Tågföretagen anser vidare att den kompletterande lagstiftningen bör ge marknadskontrollmyndigheten ett tydligt uppdrag att, i samverkan med Transportstyrelsen och ERA, inhämta och vidareförmedla kommissionens vägledning om CRA:s tillämplighet på järnvägssektorn.

Administrativa och ekonomiska konsekvenser

Efterlevnaden av cyberresiliensförordningen medför ökade administrativa och organisatoriska krav för järnvägsföretag, bland annat genom behov av nya processer, ökad dokumentation och tillgång till cybersäkerhetskompetens. För mindre och medelstora järnvägsföretag finns en särskild risk för oproportionerliga kostnader och ökat beroende av externa konsulter. Detta kan påverka konkurrensneutralitet och förutsägbarheten i verksamheten.

Tillsyn och regelefterlevnad

Förordningen innebär att järnvägsföretag, direkt eller indirekt, kan komma att beröras av marknadskontroll och tillsyn samt av sanktionsbestämmelser vid bristande efterlevnad. Då järnvägsföretag redan omfattas av krav enligt

järnvägslagstiftningen, NIS2 och annan säkerhets- och beredskapsreglering är risken för överlappande eller svåröverskådliga regelkrav påtaglig om samordningen mellan regelverk inte säkerställs.

Järnvägsföretag verkar redan inom ett sammansatt regelverk som inkluderar NIS2-direktivet (i egenskap av väsentliga entiteter), järnvägssäkerhetslagen, Transportstyrelsens föreskrifter samt de tekniska specifikationerna för driftskompatibilitet (TSD), däribland kraven på cybersäkerhet för ERTMS i genomförandeförordning (EU) 2023/1695. Cyberresiliensförordningen tillkommer som ytterligare ett regelverk med delvis överlappande krav på riskbedömning, incidentrapportering och säkerhetsåtgärder.

Tågföretagen ser en påtaglig risk för att järnvägsföretag kommer att vara föremål för parallella tillsynsförfaranden från skilda myndigheter avseende väsentligen samma system och säkerhetsåtgärder. Hur CRA:s materiella krav förhåller sig till NIS2:s krav är en EU-rättslig fråga som inte kan regleras i nationell lagstiftning. Tågföretagen anser dock att den kompletterande lagstiftningen bör innehålla ett tydligt mandat för samordning mellan marknadskontrollmyndigheten, Transportstyrelsen och övriga berörda tillsynsmyndigheter, så att järnvägsföretag inte behöver hantera parallella och potentiellt motstridiga tillsynsförfaranden. En samordnad tillsynsmodell bör utformas i dialog med branschen innan lagstiftningen träder i kraft.

Tågföretagen uppmanar vidare den svenska regeringen att på EU-nivå verka för att kommissionen klargör hur CRA förhåller sig till NIS2 för järnvägsföretag som är väsentliga entiteter, samt aktivt verka för att kommissionen prövar om det befintliga sektorsspecifika regelverket för ERTMS och ETCS kan utgöra grund för undantag från CRA i enlighet med förordningens artikel 2.2–2.3.

Samlad bedömning

Tågföretagen delar målsättningen att stärka cybersäkerheten i produkter och system, vilket är nödvändigt för ett robust transportsystem. Samtidigt bedöms cyberresiliensförordningen få betydande konsekvenser för järnvägsföretag i form av ökade krav, kostnader och administrativ belastning. För att regelverket ska bidra till ökad motståndskraft utan att försämra järnvägens funktion och konkurrenskraft är det avgörande att:

- tillämpningen blir proportionerlig och riskbaserad,
- samordningen med befintliga regelverk, särskilt NIS2 och järnvägssäkerhetslagstiftningen, säkerställs, samt
- stöd och vägledning till företag utformas tydligt och praktiskt, med särskild hänsyn till mindre aktörer.

- den svenska regeringen på EU-nivå aktivt verkar för att kommissionen utfärdar vägledning om hur begreppen *utsläppande på marknaden, väsentlig modifiering* och tillverkaransvaret vid delad systemintegration ska tillämpas på järnvägssektorns serieleveranser och upprustningsprojekt;
- frågan om ett sektorsspecifikt undantag för järnvägssektorn enligt artikel 2.2–2.3 CRA drivs aktivt av den svenska regeringen på EU-nivå, i dialog med ERA och kommissionens DG MOVE;
- samordningen mellan marknadskontrollmyndigheten, Transportstyrelsen och övriga berörda tillsynsmyndigheter formaliseras i lag eller förordning, inte enbart i myndighetsöverenskommelser.

För Tågföretagen den xx april 2026

Lina Lagerroth
Senior Näringspolitisk expert