Infrastrukturdepartementet

Datum
2023-02-16

Diarienummer
Ä 2022-5518

Remissvar - Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Tillväxtverket arbetar för hållbar tillväxt och konkurrenskraftiga företag i alla delar av Sverige. Vi skapar förutsättningar för näringslivsutveckling, för att företagen får bättre förutsättningar med enklare och mer attraktiva villkor samt främjar en hållbar regional utveckling. Tillväxtverket utvecklar kunskap om och genomför åtgärder för små och medelstora företags affärsutveckling, bland annat med fokus på deras digitala omställning. Remissvaret är skrivet utifrån dessa utgångspunkter.

Bakgrund

Syftet med förslaget är att skapa förutsättningar för utveckling av cybersäkra produkter med digitala inslag. Produkterna ska utvecklas och produceras på ett sådant sätt att en lämplig cybersäkerhetsnivå säkerställs utifrån kalkylerade risker och att de levereras utan några kända sårbarheter som kan utnyttjas. Förslaget ska ge konsumenter relevant information om cybersäkerheten för de produkter med digitala inslag som de köper och använder.

För att cybersäkerhet ska kunna säkerställas i hela leveranskedjan måste alla ingående komponenter vara cybersäkra. I dag saknar EU-lagstiftningen obligatoriska krav för säkerheten i produkter med digitala element.

Tillväxtverkets kommentarer och synpunkter

Bra med cybersäkerhetskrav på produkter och harmonisering av lagstiftning

Tillväxtverket ser positivt på förslaget till cybersäkerhetslagstiftning för produkter med digitala inslag. Vi uppfattar målen för lagstiftningen som rimliga. En harmonisering med en övergripande gemensam lagstiftning som täcker olika perspektiv av cybersäkerhet förtydligar spelreglerna för tillverkande företag, importörer och distributörer inom unionen. Det är angeläget att krav ställs på produkterna för att skydda användare, både privatpersoner och företag. Detta ökar också rättssäkerheten. Företag behöver långsiktiga regler. Lagstiftningen kan på sikt genom tydliga krav främja digital omställning, och

tillsammans med andra stödjande åtgärder, vara avgörande för företagens digitala omställning och för företagens bibehållna konkurrenskraft.

Kunskap om konsekvenserna av lagstiftningen behövs

Det är mycket viktigt vid införandet av den nya lagstiftningen att redan från början göra en löpande översyn och uppföljning av efterlevnad, tolkning och tillämpning av regelverken samt att belysa och förstå konsekvenserna av hur lagstiftningen särskilt påverkar de små och medelstora företagen. Det är också angeläget att öka kunskapen om vilka typer av företag som på olika sätt kan omfattas av den nya lagstiftningen. Marknads-kontrollmyndigheten och dess samarbetspartner i varje medlemsland samt kommissionens cybersäkerhetsorgan ENISA kommer att här att spela en avgörande roll. Det måste säkerställas att tillräcklig och relevant kapacitet och förmåga finns hos dessa organisationer redan från start av införandet av den nya lagstiftningen.

Gränsdragningsproblematik till annan lagstiftning

Förslagen i förordningen är omfattande med cybersäkerhetskrav avseende olika produktegenskaper, sårbarhetshantering, information och instruktioner till användare, med mera. Företag uppmanas exempelvis att upprätta dokumentation över vilka komponenter som ingår i produkten eller programvaruförteckningar (paragraf 37). Dessa krav kan komma i konflikt med lagstiftning om skyddsvärd information och om företagshemligheter. EU nämner ett certifieringssystem (CE) vilket möjligen kan vara ett sätt att komma runt den här problematiken. Det är bra att förslaget tar hänsyn till det standardiserings- och certifieringsarbete som redan pågår.

Kort tid för förberedelser av informationsinsatser och annat stöd

Det är i sig bra att förordningen träder i full kraft redan efter 24 månader och att företagens rapporteringsskyldighet börjar gälla efter ett år, men samtidigt kan förberedelsearbetet och organiseringen av nationella insatser för kommunikation/information och annat stöd kräva en inkörningsperiod. Detta kan behöva beaktas särskilt.

Mångfald av lagstiftning - en utmaning för små och medelstora företag

Förslagen i direktiven kompletterar ett antal näraliggande lagstiftningar relaterat till digitalisering (och cirkulär ekonomi), exempelvis direktivet om digitalt innehåll och digitala tjänster, rättsakten om artificiell intelligens, den allmänna dataskyddsförordningen, NIS-direktivet, förslag till nytt produktansvarsdirektiv vid säkerhetsbrister och förslag till direktiv om skadeståndsansvar gällande AI samt den kommande lagstiftningen för spårbarhet och digitala produktpass.

Cybersäkerhetsförordningen adderar ytterligare till enökad komplexitet och ett utökat krav på resurser, kunskap och kompetens som kan komma att påverka de mindre företagens förmåga till anpassning och bibehållen konkurrenskraft. Sammantaget kan detta leda till onödig administration och ökade kostnader för företagen. Även om ett enskilt lagförslag i sig inte leder till enavsevärd en högre administrativ börda så leder volymen av nya regler till merarbete för företagen. Detta visar också Tillväxtverkets mätningar av företagens administrativa och andra relaterade kostnader.

Ökade krav på kunskap och kompetens hos små och medelstora företag

Små och medelstora företag ingår i många leverantörskedjor för utveckling, samarbete, köp och försäljning av produkter med hård- och mjukvara. Tillämpningen av cybersäkerhetslagstiftningen leder till ett ökat ansvar gentemot användarna av

produkterna. Detta kan komplicera olika ansvarsfrågor. Många mindre företag saknar tillräcklig kunskap och kompetens inom juridik, IT och teknik för att hantera utmaningarna av cybersäkerhetslagstiftningen. Dessutom råder en brist på marknaden av relevant expertkompetens inom cybersäkerhet. Genomförda studier och insatser av Tillväxtverket pekar just på de mindre företagens bristande förmåga att agera på och använda digital säkerhet som en konkurrensfördel.

Behov av kompetenshöjande insatser riktade till små och medelstora företag

Tillväxtverket ser ett behov av nationella åtgärder, i samarbete med olika relevanta branschorganisationer och företagsfrämjande organisationer, för att informera, vägleda och ge de små företagen relevant stöd i arbetet för att anpassa produkter till lagkraven för cybersäkerhet. Rent generellt finns behov av nya initiativ för att stötta företagens digitala omställning och där cybersäkerhet/säker digitalisering specifikt bör lyftas fram.

Beslut i detta ärende har fattats av avdelningschef Tim Brooks. Karin Östberg har varit föredragande. I handläggningen har också AnnSofi Persson-Stenborg, Steven Wall, Viktoria Dagobert Spong och enhetschef Ulf Savbäck deltagit.

Tim Brooks

Karin Östberg