|  |  |
| --- | --- |
|  |  |
| Ålands lagting | BETÄNKANDE nr 09/2024-2025 |
|  | Datum |  |
| Lag- och kulturutskottet | 2025-03-06 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | Till Ålands lagting |  |
|  |
|  |
|  |
|  |

Lag- och kulturutskottets betänkande

Landskapslag om cybersäkerhet och motståndskraft

* Landskapsregeringens lagförslag LF 13/2024-2025

INNEHÅLL

[Sammanfattning 1](#_Toc192070035)

[Landskapsregeringens förslag 1](#_Toc192070036)

[Utskottets förslag 1](#_Toc192070037)

[Utskottets synpunkter 1](#_Toc192070038)

[Lagstiftningsbehörighet 2](#_Toc192070039)

[Genomförandet på Åland 3](#_Toc192070040)

[Ärendets behandling 4](#_Toc192070041)

[Reservationer 4](#_Toc192070042)

[Utskottets förslag 5](#_Toc192070043)

Sammanfattning

Landskapsregeringens förslag

Landskapsregeringen föreslår att lagtinget antar en landskapslag om cybersäkerhet och motståndskraft.

 Syftet med lagförslaget är att inom landskapet genomföra Europaparlamentets och rådets direktiv (EU) 2022/2555 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 samt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Utskottets förslag

Utskottet föreslår att lagförslaget antas.

Utskottets synpunkter

Cybersäkerhet på Åland hanteras idag med utgångspunkt i två centrala EU-direktiv. Cybersäkerhetsdirektivet (NIS 1) antogs 2016 med syftet att höja säkerhetsnivån i nätverks- och informationssystem samt säkerställa kontinuiteten i samhällsviktiga tjänster. Den snabba digitala omställningen och en utvidgad hotbild innebar att ett reviderat cybersäkerhetsdirektiv (NIS 2) antogs 2022. Direktivet medför skärpta krav på riskhantering, säkerhetsåtgärder och incidentrapportering. Cybersäkerhetsdirektivet omfattar både offentliga och privata verksamhetsutövare inom ett brett spektrum av sektorer, såsom energi, transporter, bankverksamhet, digital infrastruktur och flera andra områden. Direktivet är utformat som ett minimidirektiv, vilket innebär att medlemsstaterna har möjlighet att införa strängare regler om så önskas, men de måste följa de gemensamma minimikraven. Syftet med lagstiftningen är att implementera ett enhetligt regelverk som inte bara stärker cybersäkerheten och motståndskraften hos kritisk infrastruktur, utan även ökar tilliten till digitala tjänster i takt med den fortsatta digitaliseringen.

Motståndskraftsdirektivet (CER), som antogs 2022, syftar till att säkerställa att samhällsviktiga tjänster tillhandahålls oavbrutet inom EU:s inre marknad. Direktivet ska stärka kritiska verksamhetsutövares förmåga att förebygga, skydda, reagera på, stå emot, begränsa, anpassa sig till och återhämta sig från incidenter. Eftersom kritisk infrastruktur och tjänster är alltmer sammankopplade och ofta gränsöverskridande, har det ansetts motiverat med en harmoniserad EU-ram med minimiregler som säkerställer en enhetlig skyddsnivå. Direktivet omfattar ett brett spektrum av sektorer, exempelvis energi, transport, bankverksamhet, hälso- och sjukvård, digital infrastruktur och offentliga förvaltningar. Direktivet fastställer både skyldigheter för medlemsstaterna och för de identifierade kritiska verksamhetsutövarna. För att möjliggöra detta inrättas behöriga myndigheter, gemensamma kontaktpunkter samt nationella och gränsöverskridande samarbetsmekanismer som bland annat innefattar riskbedömningar, incidentrapportering, standardisering, tillsyn, stödåtgärder och bakgrundskontroller. Direktivet avser minska risken för störningar och skapa förutsättningar för att samhällets kritiska tjänster kan fortsätta fungera även vid större incidenter.

Lagstiftningsbehörighet

På Åland implementerades det första cybersäkerhetsdirektivet (NIS 1) inom ramen för rikets lagstiftningsbehörighet, vilket innebar att direktivet införlivades i den relevanta nationella sektorsspecifika lagstiftningen. Detta ledde till att de berörda verksamhetsutövarna tillämpade befintliga, sektorbaserade regler, medan tillsynen av cybersäkerheten fördelades på flera nationella myndigheter med ansvar för respektive sektor. Den utvidgade globala hotbilden och den ökade digitaliseringen har gjort det nödvändigt med ett mer omfattande och samordnat regelverk på EU-nivå. Det nya cybersäkerhetsdirektivet (NIS 2) ställer tydligare krav på riskhantering och incidentrapportering samt ökat samarbete både nationellt och mellan EU:s medlemsstater. Med den nya EU-lagstiftningen har landskapsregeringen bedömt att rättsområdena till stor del faller inom landskapets lagstiftningsbehörighet. Genom en åländsk fulltextlag implementeras bägge EU-direktiv på en gång. Med den föreslagna lagen sker en övergång från en tidigare, sektorsspecifik modell till en sammanhållen horisontell lagstiftning.

 Utskottet konstaterar att lagstiftningsbehörigheten är den centrala frågan i lagstiftningsförslaget. Landskapsregeringen redogör för detta utförligt i den allmänna motiveringen till lagförslaget. När det gäller EU:s cybersäkerhetsdirektiv och motståndskraftsdirektiv framgår det att, utöver de specifika undantag som enligt självstyrelselagen tillhör rikets behörighet (såsom bankverksamhet, finansmarknadsinfrastruktur, kärnkraft och lufttrafik), ligger ansvaret för att genomföra direktivens bestämmelser inom landskapets lagstiftningsbehörighet. Vidare redovisas hur delad behörighet, i de ärenden där unionsrätten föreskriver nationella åtgärder, medför att Åland ska samråda med riket och i vissa fall även direkt med EU-kommissionen.

 Utskottet konstaterar att landskapsregeringen har gjort ett grundligt arbete i att utreda lagstiftningsbehörigheten för de komplexa politikområdena cybersäkerhet och motståndskraft. EU-rätten har ändrats sedan det första cybersäkerhetsdirektivet (NIS 1) och vad som räknas till behörighetsområdet televäsende har ett annat innehåll idag än på 1980- och 1990-talet när arbetet med nuvarande självstyrelselag pågick. Utskottet kan därför instämma i landskapsregeringens bedömning att lagstiftningen i stort torde falla inom landskapets behörighet. Självstyrelselagen 18 § 27 fastställer att angelägenheter som inte uttryckligen är landskapets behörighet, kan hänföras till landskapet enligt grundsatserna i självstyrelselagen.

 Utskottet understryker att landskapets lagstiftningsbehörighet är exklusiv. Inom områden där landskapet har lagstiftningsbehörighet har riket inte rätt att utöva lagstiftande makt eller utfärda förvaltningsdirektiv. Lagförslaget är av horisontell struktur och berör flera samhällssektorer inom landskapets behörighet, varför utskottet anser att landskapsregeringens bedömning av behörighetsfördelningen följer självstyrelselagens grundsats.

 Utskottet noterar att det finns behov av en pragmatisk tillämpning av reglerna, och ser fram för sig ett behov av överenskommelseförordningar. Att säkerställa att regler och information om cybersäkerhet och motståndskraft kommuniceras på svenska tryggas, är enligt utskottet avgörande för att både myndigheter och verksamheter ska agera på korrekt information. Språklig tillgänglighet är en form av rättssäkerhet och ett viktigt verktyg för att införliva effektiv cybersäkerhet och motståndskraft. Självstyrelselagen ålägger myndigheterna att säkerställa att medborgarna får relevant information på svenska, en princip som utskottet anser särskilt viktigt i kriser eller hotfulla situationer och varför en åländsk lag har fördelar.

Genomförandet på Åland

Insulära områden som Åland är särskilt beroende av robust digital och fysisk infrastruktur för att upprätthålla kommunikation, tjänsteleveranser och samhällsviktig verksamhet. Utskottet konstaterar att regelverk för cybersäkerhet och motståndskraft är viktigt för att skydda kritisk infrastruktur mot cyberattacker och störningar, och säkerställa att verksamheter kan fortsätta fungera även under påfrestande omständigheter.

Motståndskraftsdirektivet fokuserar på att säkerställa att kritiska enheter har robusta beredskaps- och kontinuitetsplaner för att minimera störningar. Regelverket på EU-nivå inkluderar krav på riskbedömning och hantering av potentiella störningar, med särskilt fokus på att skydda samhällsviktiga tjänster mot både digitala och fysiska hot. En viktig aspekt är att om en organisation omfattas av motståndskraftsdirektivet, så måste den även följa de krav som ställs enligt cybersäkerhetsdirektivet, vilket innebär ett dubbelt ansvar för både cybersäkerhet och övergripande motståndskraft. Cybersäkerhetsdirektivet gäller både offentliga och privata verksamhetsutövare som är verksamma inom EU och omfattar i huvudsak medelstora och större företag. Direktivet täcker 18 sektorer som delas in i två grupper: 1) högkritiska sektorer exempelvis energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning och rymden, samt 2) andra kritiska sektorer som omfattar bland annat post- och budtjänster, avfallshantering, tillverkning av kemikalier och livsmedel samt digitala leverantörer. Direktivet innehåller bestämmelser om att även mindre verksamhetsutövare kan omfattas om de exempelvis är den enda leverantören av en kritisk tjänst eller om en störning kan få betydande konsekvenser för människors säkerhet och den ekonomiska funktionen.

 Utskottet har erfarit att antalet verksamhetsutövare på Åland som kommer omfattas av reglerna blir avgörande. Ålands insulära läge och infrastruktur som sträcker sig mellan skärgårdskommuner och fasta Åland, samt mellan Åland och Sverige respektive Finland, gör att flertalet mindre verksamhetsutövare kan identifieras som samhällsviktiga aktörer.

 Utskottet konstaterar att kraven som ställs i lagförslaget blir betungade för mindre verksamhetsutövare, och förväntar sig att landskapsregeringen genomför reglerna på ett proportionerligt sätt som inte snedvrider åländska aktörers konkurrenskraft samt tillhandahåller stöd för verksamheter att efterleva reglerna.

Landskapsregeringen föreslår att de åländska myndigheterna har ansvar för tillsyn och genomförande av de åtgärder som direktiven ställer.

 Utskottet konstaterar att med lagstiftningsbehörighet följer förvaltningsuppgifter och de åtföljande kostnaderna för dessa. Det föreslagna regelverket innebär stort ansvar för landskapsregeringen att ombesörja riskhantering, säkerhetsåtgärder och incidentrapportering för att hantera de alltmer omfattande och sofistikerade cyberattackerna, samt en ökad administrativ börda genom kravet på tillsyn. Att landskapsregeringens enheter ska vara både rådgivande organ och sköta tillsynen är enligt utskottet problematiskt.

 Utskottet instämmer i landskapsregeringens bedömning att lagförslaget kommer leda till ökade kostnader både för berörda verksamhetsutövare och för landskapsregeringen själv. Utskottet har dock erfarit att verksamhetsutövare redan idag efterlever mycket av regelverket genom att arbeta med en säker IT-miljö och goda rutiner kring incidenter.

 Utskottet har erfarit att åländska verksamhetsutövare idag köper tjänster för att upptäcka cyberhot av leverantörer utanför Åland. Utskottet konstaterar att sådana tjänster och ingångna avtal inte påverkas av att EU-reglerna implementeras genom en åländsk lag.

 Utskottet noterar att landskapsregeringen framhåller att lagförslaget anpassar implementeringen av EU-direktiven till de lokala förutsättningarna på Åland samt håller sig nära reglernas minimikrav. Utskottet har dock erfarit att det föreslagna lagförslaget vid tillfällen inför strängare regler än vad som är nödvändigt. Enligt utskottets mening är det viktigt att landskapsregeringen gör en proportionerlig bedömning vid identifieringen av verksamhetsutövare som omfattas av regelverket.

Ärendets behandling

Lagtinget har den 15 januari 2025 begärt lag- och kulturutskottets yttrande i ärendet.

* 1. Utskottet har i ärendet hört ministern Ingrid Zetterman, digitaliseringschefen Jani Sjölund, lagberedaren Rickard Stenman, lagberedningschefen Hans Selander, rättschefen Michaela Slotte, rättssakkunnige Rasmus Lindqvist, juristen Camilla Hägglund-Palmqvist, utskottsordföranden Ålands näringsliv Tommy Sjöblom, VD Ålands vatten Sölve Högman, Förvaltningschefen Ålands gymnasium Ronny Holmström, IT-chefen Mariehamns Energi Jim Tommiska, VD Ålands Elandelslag David Karlsson, VD Kraftnät Åland Conny Rosenberg, förbundsdirektören Ålands kommunförbund Minna Hellström, VD Mariehamns Hamn Alef Jansson, VD Långnäs Hamn Ronny Eriksson, styrelsemedlem Långnäs Hamn Robin Weiss, direktörn The European Centre of Excellence for Countering Hybrid Threats Teija Tiilikainen, samt avdelningschefen Cybersäkerhetscentret Transport- och kommunikationsverket Kristian Selén.

   Utskottet har fattat beslut efter omröstning utfallit (4-3), varvid beslutet biträddes av ordföranden Harry Jansson, vice ordföranden Sandra Listherby, samt ledamöterna Peter Lindbäck och Henrik Löthman. Ledamöterna Veronica Thörnroos, Anders Holmberg och Johan Lindström röstade emot.

 I ärendets avgörande behandling deltog ordföranden Harry Jansson, vice ordföranden Sandra Listherby samt ledamöterna Anders Holmberg, Peter Lindbäck, Johan Lindström, Henrik Löthman och Veronica Thörnroos.

Reservationer

Följande reservationer har fogats till betänkandet:

Ledamoten Veronica Thörnroos samt ledamöterna Anders Holmberg och Johan Lindström har inlämnat en reservation tillsammans.

Utskottets förslag

Med hänvisning till det anförda föreslår utskottet

att lagtinget antar lagförslaget i oförändrad lydelse.

|  |
| --- |
| Mariehamn den 6 mars 2025 |
| Ordförande | Harry Jansson  |
| Sekreterare | Julia Lindholm |