

Helsingfors/Mariehamn 26.5.2025

Nr 22/25

Hänvisning Ålands lagtings skrivelse
17.3.2025, nr 38/2025.

Till Justitieministeriet

Ärende Utlåtande över landskapslag om cybersäkerhet och motståndskraft, antagen av lagtinget 17.3.2025

Landskapslagens huvudsakliga innehåll

Landskapslagen om cybersäkerhet och motståndskraft syftar till att 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 (*cybersäkerhetsdirektivet*) samt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (*motståndskraftsdirektivet*).

Landskapslagen är uppdelad i nio kapitel. I kapitel 1 ingår allmänna bestämmelser. Enligt 1 § är syftet med landskapslagen att uppnå en hög cybersäkerhetsnivå samt uppnå en hög grad av motståndskraft och säkerställa tillhandahållandet av samhällsviktiga tjänster. I 2 § ingår 51 punkter som innehåller definitioner av centrala begrepp i lagen.

I kapitel 2 ingår bestämmelser om lagens tillämpningsområde. I 3 § föreskrivs om de verksamhetsutövare lagen ska tillämpas på. I 4 § bestäms hur tillämpningsområdet har avgränsats i förhållande till verksamhetsutövarna. I kapitlet finns också bestämmelser om landskapslagens förhållande till annan lagstiftning. Det ingår också bestämmelser om jurisdiktion, territorialitet och gränsöverskridande verksamhetsutövare.

I kapitel 3 finns bestämmelser om klassificering, identifiering och informering av verksamhetsutövare. Bland annat följer av 10 § att landskapsregeringen ska identifiera verksamhetsutövare vilka omfattas av förteckningar i bilagan till motståndskraftsdirektivet som kritiska alternativt väsentliga eller viktiga verksamhetsutövare. Av 11 § följer en skyldighet för olika verksamhetsutövare att anmäla, underrätta eller lämna uppgifter till landskapsregeringen. I 12 § föreskrivs om att landskapsregeringen ska överlämna uppgifter till ansvarig riksmyndighet och kommissionen i syfte att uppfylla det som följer av cybersäkerhetsdirektivet.

I kapitel 4 finns bestämmelser om kritiska verksamhetsutövares skyldigheter. I kapitel 5 finns bestämmelser om väsentliga och viktiga verksamhetsutövares skyldigheter. I kapitel 6 finns bestämmelser om cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter. Landskapsregeringen ska fungera både som cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter. Cyberkrishanteringsmyndigheten ansvarar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Enheten för hantering av cybersäkerhetsincidenter ansvarar för hanteringen av cybersäkerhetsincidenter på Åland. I 27 § föreskrivs om krav på enheten för hantering av cybersäkerhetsincidenter och dess uppgifter.

I kapitel 7 finns främst bestämmelser om landskapsregeringens informationsansvar i samband med incidenter och cybersäkerhetsincidenter. I kapitel 8 föreskrivs om tillsyn och efterlevnadskontroll. Landskapsregeringen ska fungera som tillsynsmyndighet. I kapitlet finns bestämmelser bland annat om landskapsregeringens rätt att få information och utföra inspektioner, internationell handräckning, vite och administrativa påföljdsavgifter. I kapitel 9 finns särskilda bestämmelser.

Lagstiftningsbehörigheten

Landskapslagen syftar till genomförandet av EU-rättsliga förpliktelser. Med anledning härav konstaterar Ålandsdelegationen att enligt självstyrelselagens 59 b § 1 mom. är lagstiftningsbehörigheten och behörigheten i förvaltningsärenden för Ålands del fördelad mellan landskapet och riket på det sätt som anges i självstyrelselagen när åtgärder vidtas i Finland med anledning av beslut som har fattats inom Europeiska unionen. Det förhållandet att medlemskapet i Europeiska unionen och att en del av lagstiftnings- och förvaltningsbehörighet som avser landskapet utövas på EU-nivå påverkar inte behörighetsfördelningen mellan landskapet och riket när unionsrätten genomförs på nationell nivå (RP 18/2002 rd, s. 18).

Enligt landskapslagens 1 § är syftet med lagen att uppnå en hög cybersäkerhetsnivå samt uppnå en hög grad av motståndskraft och säkerställa tillhandahållandet av samhällsviktiga tjänster. Definitionen av cybersäkerhet följer av artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) 526/2013. I förordningens artikel 2.1 har cybersäkerhet definierats som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

Definitionen av nätverks- och informationssystem följer av artikel 6.1 i cybersäkerhetsdirektivet som har beaktats i landskapslagens 2 § 4 punkt. Definitionen av nätverks- och informationssystem är vid och omfattar: a) ett elektroniskt kommunikationsnät, i betydelsen ett system för överföring, oberoende av om det bygger på en permanent infrastruktur eller en centralt administrerad kapacitet eller inte, och i tillämpliga fall utrustning för koppling eller dirigerering samt andra resurser, inbegripet nätelement vilka inte är aktiva, vilket medger överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier, däribland satellitnät, fasta nät, kretskopplade och paketkopplade, inbegripet internet, och mobilnät, elnätssystem i den utsträckning dessa används för signalöverföring, nät för radio- och tv-utsändning samt kabel-tv-nät, oberoende av vilken typ av information som överförs, b) en enhet eller en grupp enheter vilka är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller c) digitala uppgifter vilka lagras, behandlas, hämtas eller överförs med sådana hjälpmedel vilka omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas.

Cybersäkerhet omnämns inte vid fördelningen av lagstiftningsbehörigheten mellan landskapet och riket i självstyrelselagen. Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148, som cybersäkerhetsdirektivet upphäver, var att bygga upp cybersäkerhetskapaciteten i hela unionen, begränsa hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt. Målsättningen är bred.

Enligt 18 § 6 punkten i självstyrelselagen hör allmän ordning och säkerhet med de undantag som nämns i 27 § 27, 34 och 35 punkten till landskapets lagstiftningsbehörighet. Enligt de sistnämnda punkterna hör bl.a. ordningsmaktens verksamhet för tryggnad av statens säkerhet, försvarstillstånd och beredskap inför undantagsförhållanden till rikets lagstiftningsbehörighet. Enligt inrikesministeriets definition

är cybersäkerhet ett av delområdena inom den nationella säkerheten. Avsikten är att trygga samhällets funktionsförmåga genom att skydda samhället, som digitaliseras i allt snabbare takt, mot fientlig cyberpåverkan och underrättelseinhämtning som avser datanät. Utmärkande för cyberhot mot den nationella säkerheten är att de är statliga cyberhot som utnyttjar datanät och som riktar sig mot till exempel kritisk infrastruktur, statens beslutsfattande och ledning eller landets försvar. Även cyberbrottslingar attackerar dock i större utsträckning till exempel aktörer inom hälso- och sjukvårdssektorn och energisektorn med utpressningsprogram. Dessutom använder statliga aktörer grupper av cyberbrottslingar som underleverantörer för att hemlighålla sin egen medverkan.¹

Enligt artikel 4.2 i fördraget om Europeiska unionen ska unionen respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar. EU-domstolen har erinrat om att det av fast rättspraxis framgår att även om det ankommer på medlemsstaterna att besluta om de åtgärder som är ägnade att säkerställa allmän ordning inom deras respektive territorier samt deras inre och yttre säkerhet, är sådana åtgärder emellertid inte fullständigt undantagna från unionsrättens tillämpning. Domstolen konstaterade att det föreskrivs uttryckliga undantag i fördraget som är tillämpliga på situationer som kan äventyra lag och ordning samt allmän säkerhet enbart i artiklarna 36, 45, 52, 65, 72, 346 och 347 FEUF, som avser exceptionella och väl avgränsade fall. Det går inte härav att sluta sig till att det skulle finnas ett generellt och konstitutivt förbehåll i fördraget som innebär att alla åtgärder som vidtas med hänvisning till lag och ordning eller allmän säkerhet faller utanför unionsrättens tillämpningsområde. Räckvidden av de krav som följer av upprätthållandet av lag och ordning och den inre säkerheten kan således inte bestämmas unilateralt av respektive medlemsstat, utan någon kontroll från unionsinstitutionernas sida (dom av den 2 april 2020 i de förenade målen C-715/17, C-718/17 och C-719/17, Europeiska kommissionen mot Republiken Polen m.fl., ECLI:EU:C:2020:257, punkterna 143 och 146).

Både cybersäkerhets- och motståndskraftsdirektivet har antagits med hänvisning till artikel 114 om den inre marknadens funktion i fördraget om Europeiska unionens funktionssätt. Cybersäkerhetsdirektivets målsättning är att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Enligt skäl 3 i ingressen till cybersäkerhetsdirektivet har nätverks- och informationssystem utvecklats till ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället, vilket även gäller vid

¹ Inrikesministeriet, 'Cybersäkerhet som ett led i den nationella säkerheten', <https://intermin.fi/sv/nationell-sakerhet/cybersakerhet>.

gränsöverskridande utbyten. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana incidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera ekonomisk förlust, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.

Ålandsdelegationen konstaterar att cybersäkerhet, informationssäkerhet och dataskydd delvis överlappar varandra. I sammanhanget bör beaktas vilken inriktning och vilket syfte landskapslagstiftningen har i förhållande till nätverks- och informationssystemen. Det ingår i många avseenden i landskapets lagstiftningsbehörighet att anta lagstiftning som berör nätverks- och informationssystem, till exempel används dessa system i förvaltningsförfarandet inom landskapets behörighet. Därtill bör det beaktas att 1 § i den nyligen antagna informationshanteringslagen för Åland anger att lagen syftar till att säkerställa en enhetlig och kvalitativ hantering samt informationssäker behandling av myndigheternas informationsmaterial så att offentlighetsprincipen förverkligas. I den lagens tredje kapitel föreskrivs om informationssäkerhet. Informationssäkerhet syftar till att skydda information och data som en organisation hanterar, både digital och fysisk information. Dessa bestämmelser har ansetts falla inom landskapets lagstiftningsbehörighet (ÅD-utlåtande 11/25 och Högsta domstolens utlåtande 7.4.2025, KKO-HD/258/2025). Lagstiftningens tillämpningsområde avgränsades till myndigheters behandling av informationsmaterial.

Lagstiftningen om dataskydd ska skydda de personuppgifter som behandlas i nätverks- och informationssystem. Dataskyddslagstiftningen är också tillämplig inom ramen för landskapslagens tillämpningsområde. Dataskydd eller behandling av personuppgifter omnämns inte vid uppdelningen av lagstiftningsbehörigheten mellan landskapet och riket i självstyrelselagen. Lagstiftningsbehörigheten bör därför bedömas utgående från de rättsområden landskapslagstiftningen kan beröra (Högsta domstolens utlåtande 5.3.2019, OH2019/11). Tillämpningen av landskapslagstiftningen om dataskydd och skydd av personuppgifter utsträcker sig också till landskapets behörighet över verksamhet inom den privata sektorn (Högsta domstolens utlåtande 1.8.2019, OH2019/130). Landskapslagen om cybersäkerhet och motståndskraft fokuserar mera på skyddet av nätverks- och informationssystem, dvs. de tekniska och organisatoriska lösningar som utnyttjas vid behandlingen av personuppgifter.

Ålandsdelegationen anser att behörighetsfördelningen i fråga om cybersäkerhet bör bedömas med utgångspunkt i vilka rättsområden landskapslagstiftningen kan beröra. Enligt Ålandsdelegationen kan landskapslagstiftningen om cybersäkerhet också komma att utsträckas till privata verksamhetsutövare till den del dessa verkar inom rättsområden som hör till landskapets lagstiftningsbehörighet. Enligt 18 § 22 punkten i självstyrelselagen tillkommer lagstiftningsbehörigheten gällande näringsverksamhet, med vissa undantag, landskapet.

Det bör även beaktas att landskapslagstiftning om cybersäkerhet behöver ta hänsyn till behörighetsgränsen och möjliga koordineringsbehov i förhållandet till området för televerksamhet som enligt 27 § 40 punkten i självstyrelselagen hör till rikets lagstiftningsbehörighet. I lagstiftningskontrollen har bedömts hur landskapslagstiftning har förhållit sig till informationssamhällsbalken. Högsta domstolen har hänvisat till att informationssamhällsbalken gäller både allmän televerksamhet och överförings- och sändningstjänster i masskommunikationsnät. Domstolen torde ha haft som utgångspunkt att den televerksamhet som det föreskrivs om i informationssamhällsbalken (numera lagen om tjänster inom elektronisk kommunikation, FFS 917/2014) hör till rikets lagstiftningsbehörighet (Högsta domstolens utlåtande 3.3.2017, OH2017/8). Tidigare har Ålandsdelegationen konstaterat att domännamnen berör närmast området för televerksamhet, men att dessa är enligt 27 § 42 punkten i självstyrelselagen att hänföra till rikets lagstiftningsbehörighet (se ÅD-utlåtandena 5/05 och 19/16). I lagen om tjänster inom elektronisk kommunikation föreskrivs om den åländska toppdomänen. Tillämpningen i landskapet av lagen om tjänster inom elektronisk kommunikation begränsas av att landskapet har lagstiftningsbehörigheten gällande rätten att utöva rundradio- och televisionsverksamhet inom landskapet enligt 18 § 20 punkten i självstyrelselagen.

I riket har cybersäkerhetsdirektivet främst genomförts genom antagandet av cybersäkerhetslagen (FFS 124/2025), men också genom ändringar i annan lagstiftning (se RP 57/2024 rd). I fråga om den offentliga sektorn har direktivet genomförts i riket genom ändring av lagen om informationshantering inom den offentliga förvaltningen (FFS 906/2019). Riksdagen har i maj 2025 fattat beslut om antagandet av lagstiftning som genomför motståndskraftsdirektivet (RSv 47/2025 rd). Landskapslagen syftar till ett genomförande av såväl cybersäkerhets- som motståndskraftsdirektivet. Lagstiftningsmodellen skiljer sig från den i riket eftersom landskapslagen ska genomföra både cybersäkerhets- och motståndskraftsdirektivet samtidigt som den också ska tillämpas i förhållande till den offentliga förvaltningen inom landskapets behörighet. I vissa avseenden utesluter unionslagstiftningen parallella lösningar inom landskapets behörighet. Enligt artikel 7 i cybersäkerhetsdirektivet ska varje medlemsstat anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla

en hög cybersäkerhetsnivå. Av artikel 4 i motståndskraftsdirektivet följer motsvarande krav på att medlemsstaterna antar en strategi. I självstyrelselagens 59 b § 2 mom. föreskrivs om hur landskapsmyndigheterna och riksmyndigheterna ska gå till väga om endast en åtgärd kan vidtas i medlemsstaten i ett förvaltningsärende där både landskapet och riket har behörighet (jfr ÅD-utlåtande 5/19, s. 2–3).

I landskapslagens 2 kap. föreskrivs om lagens tillämpningsområde. I landskapslagens 3 § 1 mom. föreskrivs om de verksamhetsutövare som lagen ska tillämpas på. Lagen ska tillämpas på verksamhetsutövare om de eller deras verksamhet, vilken inte är ringa eller sporadisk, omfattas av förteckningarna i bilagorna I eller II till cybersäkerhetsdirektivet och villkor uppräknade i någon av 1–8 punkterna är uppfyllda. Enligt 2 § 41 punkten definieras en verksamhetsutövare som en juridisk eller fysisk person, enskild eller offentlig, vilken bedriver verksamhet. Av 3 § 1 mom. 7 punkten följer att lagen tillämpas i förhållande till offentliga verksamhetsutövare. Enligt 2 § 42 punkten definieras en offentlig verksamhetsutövare som landskapsregeringen och under denna lydande myndigheter och affärsverk, med undantag för Ålands polismyndighet. Enligt förarbetena omfattar lagens tillämpningsområde offentliga verksamhetsutövare, vilka i lagen definieras som landskapets myndigheter, och privata verksamhetsutövare vilka antingen klassificeras eller identifieras av tillsynsmyndigheten som kritiska, väsentliga eller viktiga verksamhetsutövare, utifrån de i direktiven angivna kriterierna för detta (lagförslag nr 13/2024–2025, s. 41). Enligt 3 § 2 mom. ska lagen även tillämpas på verksamhetsutövare om de eller deras verksamheter omfattas av bilagan till motståndskraftsdirektivet och har identifierats som kritiska verksamhetsutövare.

I 4 § avgränsas lagens tillämpningsområde. Enligt detaljmotiveringen syftar 1–3 mom. till ett utnyttjande av det nationella handlingsutrymmet enligt cybersäkerhets- och motståndskraftsdirektivet. Avgränsningarna i paragrafens 4 och 5 mom. syftar till att genomföra enskilda bestämmelser i dessa direktiv (lagförslag nr 13/2024–2025, s. 68). Vid en närmare jämförelse framkommer att paragrafen motsvarar i många avseenden bestämmelserna i 4 § i cybersäkerhetslagen (FFS 124/2025). Enligt 1 mom. ska de angivna skyldigheterna inte tillämpas på verksamhetsutövares verksamhet eller tjänster vilka tillhandahålls inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. Enligt 27 § 23 och 34 punkterna i självstyrelselagen tillhör lagstiftningsbehörigheten inom dessa områden huvudsakligen riket. Allmän ordning och säkerhet, med de undantag som nämns i 27 § 27, 34 och 35 punkten, hör till landskapets lagstiftningsbehörighet enligt 18 § 6 punkten i självstyrelselagen. Av 4 § 3 mom. följer att landskapslagen ska delvis tillämpas på verksamhetsutövares verksamhet eller tjänster vilka tillhandahålls inom de områden som nämns i 1 mom. En sådan tillämpning avgränsas till områden inom landskapets lagstiftningsbehörighet.

I 5 § finns bestämmelser om förhållandet till annan lagstiftning. Enligt 1 mom. ska lagen enbart tillämpas på verksamhetsutövare vilka omfattas av bestämmelserna i detta kapitel till den del som dessa bedriver verksamhet eller tillhandahåller tjänster inom ramen för Ålands lagstiftningsbehörighet. Eftersom lagstiftningen om cybersäkerhet faller både inom landskapets och rikets lagstiftningsbehörighet kan verksamhetsutövare på Åland vara föremål för både unions-, riks- och landskapslagstiftning. Fördelningen av lagstiftningsbehörighet gällande cybersäkerhet följer av vilket rättsområde som verksamheten berör. För verksamhetsutövarna kan det vara oklart till vilken del verksamheten är föremål för landskaps- respektive rikslagstiftning. Detta kan förutsätta att kompletterande rådgivning ges i landskapet i syfte att klargöra när landskapslagen är tillämplig.

Av 5 § 2 mom. följer att om det i sektorsspecifika unionsrättsakter, någon annan lag eller bestämmelser eller föreskrifter vilka har utfärdats med stöd av någon annan lag föreskrivs att kritiska verksamhetsutövare ska vidta åtgärder för att stärka sin motståndskraft eller att en väsentlig eller viktig verksamhetsutövare ska vidta åtgärder för cybersäkerhet eller rapportera betydande cybersäkerhetsincidenter vilka avviker från denna lag, och dessa krav har minst samma verkan som motsvarande skyldigheter vilka fastställs i denna lag, ska dessa tillämpas i stället för motsvarande bestämmelser i denna lag, inbegripet sammanhängande bestämmelser om tillsyn och efterlevnadskontroll i 8 kap. I detaljmotiveringen anges att branschspecifika krav som finns i en unionsrättslig, nationell eller åländsk lag eller i bestämmelser eller föreskrifter som utfärdats med stöd av en sådan ska tillämpas i stället för motsvarande bestämmelser i landskapslagen (lagförslag nr 13/2024–2025, s. 69). Ålandsdelegationen konstaterar dock att en riksförfattning inte tillämpas direkt inom landskapets lagstiftningsbehörighet, men s.k. blankettlagstiftning kan ligga till grund för riksförfattningars tillämpning inom landskapets lagstiftningsbehörighet. Förenligheten med självstyrelselagen förutsätter att detta beaktas i samband med tillämpningen av 5 § 2 mom.

I landskapslagens 6 § finns bestämmelser om jurisdiktion, territorialitet och gränsöverskridande verksamhetsutövare. Genom bestämmelserna genomförs artikel 26 i cybersäkerhetsdirektivet. Enligt 6 § 1 mom. ska lagen tillämpas på verksamhetsutövare vilka är etablerade och bedriver verksamhet eller tillhandahåller tjänster på Åland. I paragrafen föreskrivs också om tillämpningen av lagen då verksamhetsutövarna inte är etablerade på Åland eller då de också är etablerade på annat ställe än Åland. Verksamhet som sker genom nätverks- och informationssystem är av en särskild karaktär eftersom den är gränsöverskridande och inte avgränsad till ett visst territorium. Därför kan upprätthållandet av en hög cybersäkerhetsnivå förutsätta åtgärder i förhållande till verksamhet med ursprung i ett annat territorium.

Utgångspunkten är att landskapets lagstiftningskompetens endast omfattar landskapets område (Högsta domstolens utlåtande 1.8.2019, OH2019/131). I vissa landskapslagar som har varit föremål för lagstiftningskontroll har ingått bestämmelser om tillämpligheten på aktörer etablerade utanför Åland (se till exempel 2 § 2 mom. i den av lagtinget 25.4.2022 antagna landskapslagen om näringsrätt och näringstillstånd, som inte satts i kraft, och ÅD-utlåtande 20/22, s. 2). Högsta domstolen har också tagit ställning till frågan om en förening som inom landskapet Åland hade ett giltigt tillstånd att föranstalta penningspel på Internet hade utsträckt verksamheten till riket. Domstolen drog slutsatsen att även om spelservern varit belägen utanför riket och administrationen av spelen likaså ägt rum utanför riket måste föreningens åtgärder i syfte att möjliggöra och främja speldeltagande i riket anses innebära att lotteriet har föranstaltats i riket (Högsta domstolens dom 2005:27, stycke 12–19). På motsvarande sätt kan landskapslagarnas tillämpning omfatta aktörer vars gränsöverskridande verksamhet som sker genom nätverks- och informationssystem utsträcks till Åland.

Enligt 6 § 6 mom. omfattas gränsöverskridande verksamhetsutövare vilka omfattas av en annan medlemsstat i Europeiska unionens jurisdiktion men vilka tillhandahåller tjänster eller har ett nätverks- och informationssystem på Åland av denna lags bestämmelser om tillsyn och efterlevnadskontroll i 8 kap. i den mån som landskapsregeringen agerar inom ramen för en begäran om ömsesidigt bistånd. Enligt detaljmotiveringen kan landskapsregeringen på det sätt som föreskrivs i lag utföra tillsyns- och efterlevnadskontrollåtgärder som avser verksamhetsutövare etablerade i en annan medlemsstat i Europeiska unionen, om tillsynsmyndigheten i etableringsstaten begär det (lagförslag nr 13/2024–2025, s. 71). Det ömsesidiga biståndet rör samarbetet och utförandet av förvaltningsuppgifter mellan myndigheter i syfte att upprätthålla en hög cybersäkerhetsnivå. Ålandsdelegationen anser att det inte rör sig om förhållandet till utländska makter enligt 27 § 4 punkten i självstyrelselagen. Delegationen noterar att det i 6 § 6 mom. hänvisas till Europeiska unionens jurisdiktion, men cybersäkerhetsdirektivet avser medlemsstaternas jurisdiktion.

I landskapslagens 7–9 § ingår bestämmelser om klassificeringar av kritiska, väsentliga och viktiga verksamhetsutövare. Klassificeringen av de kritiska verksamhetsutövarna baserar sig på bestämmelser i motståndskraftsdirektivet medan klassificeringen av de väsentliga och viktiga verksamhetsutövarna följer av bestämmelser i cybersäkerhetsdirektivet. Enligt 10 § ska landskapsregeringen identifiera och underrätta verksamhetsutövarna om ovan nämnd klassificering. Enligt 3 mom. ska verksamhetsutövarna också underrättas om de skyldigheter som anges närmare i bestämmelsen. Ålandsdelegationen konstaterar att landskapsregeringen enbart kan klassificera och underrätta verksamhetsutövare till den del deras verksamhet faller inom landskapets lagstiftningsbehörighet. Även underrättelse av verksamhetsutövare som eventuellt är etablerade utanför Åland kan anses

falla inom ramen för landskapets behörighet (jfr Högsta domstolens utlåtande 27.12.2007 om delgivning till utlandet).

I landskapslagens 12 § finns närmare föreskrivet om landskapsregeringens informationsutlämning för förteckning och till kommissionen. Av 1–2 mom. följer landskapsregeringens skyldighet att till ansvarig riksmyndighet överlämna samtliga de uppgifter vilka den behöver för att upprätta förteckningar över kritiska, väsentliga och viktiga verksamhetsutövare. I 3–5 mom. föreskrivs närmare om landskapsregeringens informationsutlämning till kommissionen. Enligt 59 b § 4 mom. i självstyrelselagen har landskapsregeringen rätt att stå i kontakt med Europeiska gemenskapernas kommission i ärenden som hör till landskapets behörighet och som gäller verkställighet i landskapet av beslut som har fattats inom Europeiska unionen. Landskapsregeringen och statsrådet kommer närmare överens om hur statsrådet skall informeras om sådana kontakter. Enligt förarbetena kan frågor som avses i bestämmelsen t.ex. vara anmälningar som gäller offentlig upphandling, anmälningar om s.k. statligt stöd till näringslivet och verkställighet av strukturfondsprogram i landskapet med tillhörande rapporteringsskyldigheter. Bestämmelsen skall också avse svar på sådana förfrågningar som kommissionen riktar till Finland och som gäller olika ärenden, t.ex. förfrågningar om innehållet i lagstiftningen eller om myndigheternas verksamhet inom landskapets behörighetsområden (RP 18/2002 rd, s. 20). Ålandsdelegationen anser att bestämmelserna kan tas in i lagen.

I landskapslagens 4 och 5 kap. finns bestämmelser om kritiska respektive väsentliga och viktiga verksamhetsutövares skyldigheter. Bestämmelserna i 4 kap. om kritiska verksamhetsutövares skyldigheter avser att genomföra motståndskraftsdirektivets bestämmelser. Bestämmelserna i 5 kap. om väsentliga och viktiga verksamhetsutövares skyldigheter genomför cybersäkerhetsdirektivets bestämmelser. I kapitlen finns bestämmelser som är att hänföra till rikets lagstiftningsbehörighet. I en landskapslag kan enligt 19 § 3 mom. i självstyrelselagen för Åland för vinnande av enhetlighet och överskådlighet intas stadganden av rikslagstiftningsnatur som i sak överensstämmer med motsvarande stadganden i rikslag. Intagande av sådana stadganden i en landskapslag medför inte ändring i fördelningen av lagstiftningsbehörigheten mellan riket och landskapet.

I 15 § hänvisas till att i 4 kap. i säkerhetsutredningslagen (FFS 726/2014) finns bestämmelser om rätt att hos där i angiven riksmyndighet begära om säkerhetsutredning av personer i vissa fall. Syftet med den lagen är att främja möjligheterna att förebygga verksamhet som kan medföra skada för statens säkerhet, försvaret, Finlands internationella förbindelser, den allmänna säkerheten eller något annat med dessa jämförbart allmänt intresse eller enskilda ekonomiska intressen av synnerligen stor betydelse eller säkerhetsarrangemang för skyddet av dessa intressen. Säkerhetsutredning knyter huvudsakligen an till rikets lagstiftningsbehörighet och hänvisningen kan

tas in i bestämmelsen. I 17 § och 24 § föreskrivs om verksamhetsutövarnas användning av tillämpliga europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i dess nätverks- och informationssystem. Enligt 27 § 19 punkten i självstyrelselagen hör standardisering till rikets lagstiftningsbehörighet. På motsvarande sätt berör bestämmelsen i 23 § 1 mom. om verksamhetsutövarnas användning av enligt europeiska ordningar för cybersäkerhetscertifiering certifierade produkter, tjänster och processer rikets lagstiftningsbehörighet.

I 6 kap. finns bestämmelser om cyberkrishanteringsmyndigheten. Enligt artikel 9.1 i cybersäkerhetsdirektivet ska varje medlemsstat utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Enligt artikel 10.1 ska varje medlemsstat utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheterna får utses eller inrättas inom en behörig myndighet. CSIRT-enheterna ska uppfylla kraven i artikel 11.1, ska omfatta minst de sektorer, delsektorer och typer av entiteter som avses i bilagorna I och II och ska ansvara för incidenthantering i enlighet med ett tydligt fastställt förfarande.

Enligt cybersäkerhetslagen (FFS 124/2025) ska varje myndighet fungera som cyberkrishanteringsmyndighet i enlighet med de uppgifter som föreskrivits för den i lagen. Cybersäkerhetscentret vid Transport- och kommunikationsverket fungerar som koordinator mellan cyberkrishanteringsmyndigheterna och svarar i samarbete med de andra myndigheterna även för upprättandet av den nationella ramen för hantering av cybersäkerhetskriser som cybersäkerhetsdirektivet kräver för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Cybersäkerhetscentret är CSIRT-enhet för hantering av it-säkerhetsincidenter samt gemensam kontaktpunkt (RP 57/2024 rd, s. 61).

Enligt 25 § 1 mom. i landskapslagen är landskapsregeringen cyberkrishanteringsmyndighet enligt denna lag och ansvarar därmed för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Enligt landskapslagens 2 § 9 punkt definieras en storskalig cybersäkerhetsincident som en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater. Enligt 26 § 1 mom. är landskapsregeringen enhet för hantering av cybersäkerhetsincidenter enligt denna lag och ansvarar därmed för hanteringen av cybersäkerhetsincidenter på Åland. I landskapslagens 2 § 8 punkt definieras cybersäkerhetsincident som en händelse vilken undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster vilka erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

Ålandsdelegationen anser att såväl de storskaliga cybersäkerhetsincidenterna som andra cybersäkerhetsincidenter kan beröra verksamhetsutövare inom landskapets behörighet. Därför anser Ålandsdelegationen att landskapsregeringen kan till denna del fungera som cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter. Dock konstaterar Ålandsdelegationen att cybersäkerhetsincidenter är av en gränsöverskridande karaktär. Hanteringen av dem kan förutsätta samordning med behöriga riksmyndigheter i enlighet med självstyrelselagens 59 b § 2 mom. eller reglering närmare angiven i en överenskommelseförordning. Av cybersäkerhetsdirektivet och landskapslagen följer långtgående krav vad gäller bland annat tekniska lösningar och resurser hos cyberkrishanteringsmyndigheterna och enheterna för hantering av cybersäkerhetsincidenter. Lagstiftningskontrollen enligt självstyrelselagens 19 § avgränsas till en prövning av om lagtinget har överskridit sin lagstiftningsbehörighet eller landskapslagen rör rikets inre eller yttre säkerhet.

I landskapslagens 7 kap. finns bestämmelser om landskapsregeringens informationsansvar. Bestämmelserna handlar om arrangemang för informationsutbyte samt informationsansvar vid incidenter och cybersäkerhetsincidenter. Av 29 § och 30 § följer en skyldighet för landskapsregeringen att informera olika instanser om incidenter och cybersäkerhetsincidenter. I flera fall föreskrivs att landskapsregeringens information ska gå genom Finlands gemensamma kontaktpunkt. Med beaktande av att informationen framförs genom Finlands gemensamma kontaktpunkt kan bestämmelserna anses vara förenliga med självstyrelselagen.

I landskapslagens 8 kap. föreskrivs om tillsyn och efterlevnadskontroll. Enligt 31 § 1 mom. är landskapsregeringen tillsynsmyndighet enligt denna lag. Bestämmelsen genomför artikel 8.1 och 8.2 i cybersäkerhetsdirektivet och artikel 9.1 i motståndskraftsdirektivet. Tidigare har framkommit att landskapsregeringen också ska fungera som cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter. Enligt 31 § 2 mom. ska landskapsregeringen agera självständigt och oberoende i sin roll som tillsynsmyndighet. Bestämmelsen genomför artikel 31.4 i cybersäkerhetsdirektivet. Enligt denna artikel ska medlemsstaterna säkerställa att de behöriga myndigheterna, vid tillsynen av de offentliga förvaltningsentiteternas efterlevnad av detta direktiv och införandet av efterlevnadskontrollåtgärder vid överträdelser av detta direktiv, har lämpliga befogenheter att utföra dessa uppgifter och är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas. Av landskapslagen framgår inte hur det operativa oberoendet för landskapsregeringens tillsyn ska garanteras. Till denna del bör noteras att landskapsregeringen också ska utgöra en sådan offentlig verksamhetsutövare som avses i landskapslagens 3 § 1 mom. 7 punkt. Ålandsdelegationen anser att detta förhållande är problematiskt med tanke på en operativt oberoende tillsyn, men lagstiftningskontrollen avgränsar sig till en

prövning av om landskapslagstiftningen står i uppenbar konflikt med unionsrätten.

I egenskap av tillsynsmyndighet enligt 31 § 1 mom. ska landskapsregeringen utöva tillsyn och efterlevnadskontroll i enlighet med bestämmelserna i 8 kap. i landskapslagen. I 33 § finns bestämmelser om myndighetssamråd och samarbete. Landskapsregeringen förutsätts samarbeta och samråda med ett stort antal myndigheter och andra aktörer. Bestämmelserna riktar sig till landskapsregeringen och ger inte landskapsregeringen behörighet att utföra förvaltningsuppgifter inom rikets lagstiftningsbehörighet. Ålandsdelegationen anser att bestämmelserna kan tas in i landskapslagen.

Enligt 34 § kan landskapsregeringen begära att kommissionen anordnar ett rådgivande uppdrag för en kritisk verksamhetsutövare. Bland annat ska landskapsregeringen ta vederbörlig hänsyn till det rådgivande uppdragets rapport. Det rådgivande uppdraget anordnas av kommissionen i enlighet med artikel 18 i motståndskraftsdirektivet, dvs. det rådgivande uppdraget sker på unionsnivå. Tidigare framförda synpunkter om landskapsregeringens rätt att stå i kontakt med kommissionen är tillämpliga i sammanhanget. Ålandsdelegationen anser att bestämmelserna kan tas in i landskapslagen.

I 35 § föreskrivs om sakkunnigbedömning. I detta sammanhang utförs sakkunnigbedömning på nationell nivå i enlighet med lagstiftningen inom medlemsstaterna. Landskapsregeringen kan utse cybersäkerhetsexperter för deltagande vid en sakkunnigbedömning. Vid utseendet av cybersäkerhetsexperter ska beaktas de begränsningar som följer av grundlagen. Enligt självstyrelselagens 27 § 1 punkt hör stiftande, ändring och upphävande av grundlag samt avvikelser från grundlag till rikets lagstiftningsbehörighet. Enligt grundlagens 124 § kan offentliga förvaltningsuppgifter anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter.

Enligt 10 § 1 mom. grundlagen är vars och ens hemfrid tryggad. Enligt paragrafens 3 mom. kan genom lag föreskrivas om åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna skall kunna tryggas eller för att brott skall kunna utredas. Enligt grundlagsutskottets praxis bör man vid lagstiftning beträffande inspektioner beakta bestämmelserna om skyddet för hemfrid (se t.ex. GrUU 21/2010 rd, GrUU 54/2014 rd och GrUU 12/2019 rd). Grundlagsutskottet har ofta framhållit att formuleringen i 10 § 3 mom. grundlagen är absolut i det avseendet att de åtgärder som begränsar skyddet för hemfriden måste vara kopplade till ett nödvändighetskrav. För att åtgärderna ska kunna betraktas som nödvändiga

bör de vara tydligt och tillräckligt nära kopplade till någon grundlagsbestämmelse om grundläggande fri- och rättigheter (GrUU 6/2019 rd). Bestämmelserna om rätt att ingripa i de grundläggande fri- och rättigheterna ska alltid vara dels noga avgränsade, dels exakta ifråga om tillämpningsområdet (GrUU 19/2000 rd).

I 36 § finns bestämmelser om landskapsregeringens tillsyn och efterlevnadskontroll. I 36 § 1 mom. 1 punkten och 38 § 1 mom. 1 punkten föreskrivs om landskapsregeringens inspektion av kritisk infrastruktur och lokaler samt tillsyn på distans. I 41 § föreskrivs närmare om landskapsregeringens inspektioner. Enligt 41 § 2 mom. har landskapsregeringen i samband med en inspektion rätt att på tillsynsobjektet få tillträde till alla fastigheter, byggnader, lokaler, kommunikationsnät, nätverks- och informationssystem och andra system vilka är nödvändiga för inspektionen samt andra utrymmen. En inspektion får inte ske i utrymmen vilka är avsedda för boende av permanent natur. Således har i bestämmelsen beaktats de begränsningar som följer av grundlagens skydd för hemfriden.

I 41 § 4 mom. föreskrivs också om att landskapsregeringen kan, om det är nödvändigt på grund av inspektionens art eller av tekniska orsaker vilka har samband med den, begära att en annan myndighet förrättar inspektionen eller vid inspektionen anlita en annan myndighet, annat bedömningsorgan eller annan utomstående expert. I grundlagsutskottets utlåtandepraxis har det betonats att kravet på ändamålsenlighet i 124 § i grundlagen är en rättslig förutsättning som kräver bedömning från fall till fall i fråga om varje offentlig förvaltningsuppgift som föreslås bli anförtrodd någon utanför myndighetsorganisationen. Då ska man beakta bl.a. förvaltningsuppgiftens karaktär (se GrUU 44/2016 rd, s. 5 och GrUU 26/2017 rd, s. 49). Grundlagsutskottet har ansett att respekten för de grundläggande fri- och rättigheterna, rättssäkerheten och kraven på god förvaltning kan tryggas med hjälp av de berörda personernas kompetens och lämplighet (se t.ex. GrUU 5/2006 rd, s. 8/I). Grundlagsutskottet har också ansett att inspektionerna ska utföras i enlighet med de allmänna förvaltningslagarna och att de som behandlar ärendena handlar under tjänsteansvar. Dessutom har grundlagsutskottet ansett att det i regleringen av granskningar av tillsynskaraktär hos företag för klarhetens skull bör hänvisas till den allmänna bestämmelsen om inspektioner i rikets förvaltningslag (se t.ex. GrUU 44/2016 rd, s. 6). Ålandsdelegationen anser att detta har beaktats i landskapslagens 41 § 4 och 5 mom.

I 38 § 2 mom. finns bestämmelser om landskapsregeringens efterlevnadskontrollåtgärder. Enligt 3 mom. kan landskapsregeringen, om åtgärderna enligt 2 mom. är ineffektiva, fastställa en tidsfrist inom vilken verksamhetsutövaren ska ha vidtagit nödvändiga åtgärder för att avhjälpa konstaterade brister eller uppfylla landskapsregeringens krav. Enligt 4 mom. kan landskapsregeringen vidta ytterligare efterlevnadskontrollåtgärder om en enskild väsentlig verksamhetsutövare

underlåter att vidta förelagda åtgärder inom en fastställd tidsfrist enligt 3 mom. Landskapsregeringen kan 1) besluta att för viss tid, dock högst fem år, upphäva verksamhetsutövarens koncession, tillstånd eller certifiering, för en del av eller samtliga relevanta tjänster eller verksamheter, och 2) besluta att för viss tid, dock högst fem år, förbjuda en fysisk person att vara verksam som ledamot eller ersättare i en styrelse eller förvaltningsråd, verkställande direktör eller i annan därmed jämförbar ställning vid verksamhetsutövaren.

Ålandsdelegationen konstaterar att landskapsregeringens befogenheter enligt 38 § 4 mom. 1 och 2 punkterna är långtgående. Enligt 38 § 4 mom. 1 punkten kan landskapsregeringen besluta att för viss tid, dock högst fem år, upphäva verksamhetsutövarens koncession, tillstånd eller certifiering, för en del av eller samtliga relevanta tjänster eller verksamheter. Av bestämmelsen eller förarbetena framgår inte i detalj vilken typ av koncession, tillstånd eller certifiering det handlar om. Bestämmelsen motsvarar dock direktivets artikel 32.5 a punkten, enligt vilken medlemsstaterna ska säkerställa att de behöriga myndigheterna har befogenhet att tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan, eller en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten. Av 38 § 4 mom. 2 punkten följer en befogenhet för landskapsregeringen att förbjuda en fysisk person att verka i ledande ställningar vid verksamhetsutövaren (jfr cybersäkerhetsdirektivets artikel 38.5 punkt b). Bestämmelsen är utformad så att den i praktiken avser privaträttsliga sammanslutningar. Enligt 27 § 8 punkten i självstyrelselagen hör bolag och andra privaträttsliga sammanslutningar till rikets lagstiftningsbehörighet. Detta utesluter ändå inte bestämmelser som syftar till en effektiv efterlevnad av de privaträttsliga sammanslutningarnas förpliktelser fastställda inom landskapets lagstiftningsbehörighet. Ålandsdelegationen anser att bestämmelserna i 38 § kan tas in i landskapslagen.

I landskapslagens 40 § finns bestämmelser om landskapsregeringens rätt att få information. Enligt 1 mom. har landskapsregeringen rätt trots sekretessbestämmelser och andra begränsningar vilka gäller utlämnande av information att av en verksamhetsutövare få den information vilken är nödvändig för att landskapsregeringen ska kunna utföra sina tillsynsuppgifter och övriga uppgifter enligt denna lag. Enligt 2 mom. ska landskapsregeringen i begäran om information ange syftet med begäran och precisera den begärda informationen. Informationen ska lämnas ut utan dröjsmål, i den form vilken landskapsregeringen har begärt och avgiftsfritt. Ålandsdelegationen konstaterar att landskapsregeringens rätt att få information visserligen är bunden till ett krav på nödvändighet. Däremot är bestämmelserna mycket vaga med avseende på vilken information som rätten gäller. I praktiken skulle detta vara beroende av landskapsregeringens precisering enligt 2 mom. I grundlagsutskottets praxis har ansetts att en så pass omfattande rätt till information är så summariskt vag

och ospecificerad att den helt klart strider mot 10 § 1 mom. i grundlagen (GrUU 59/2010 rd, s. 4). I avsaknad av bestämmelser om avgränsningen av rätten till information är det inte heller möjligt att bedöma hur rätten förhåller sig till grundlagens 10 § 2 mom. om att brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden är okränkbar (jfr GrUU 62/2024 rd, s. 2–5). Ålandsdelegationen anser att 40 § 1 och 2 mom. utgör behörighetsöverskridningar.

I landskapslagens 42 § föreskrivs om internationell handräckning. Enligt 1 mom. ska landskapsregeringen vid tillsyn och efterlevnads-kontroll av en gränsöverskridande väsentlig eller viktig verksamhets-utövare vid behov samarbeta med och bistå andra berörda medlems-staters tillsynsmyndigheter, åtminstone i den omfattning som föreskrivs i 1–3 punkterna. I 2 mom. föreskrivs närmare om när landskapsregeringen kan avslå en begäran om ömsesidigt bistånd och i 3 mom. om samråd innan sådant avslag sker. I 4 mom. föreskrivs om gemensamma tillsynsåtgärder med andra tillsynsmyndigheter. Ovan har Ålandsdelegationen ansett att det ömsesidiga biståndet rör samarbetet och utförandet av förvaltningsuppgifter mellan myndigheter i syfte att upprätthålla en hög cybersäkerhetsnivå. Ålandsdelegationen anser att det inte rör sig om ett sådant förhållande till utländska makter som anges i 27 § 4 punkten i självstyrelselagen.

Enligt 44 § kan landskapsregeringen förena ett beslut vilket den har fattat med stöd av denna lag med vite, hot om tvångsutförande eller, i tillämpliga fall, hot om avbrytande, för vilka landskapslagen (2008:10) om tillämpning i landskapet Åland av viteslagen tillämpas. Enligt 18 § 26 punkten i självstyrelselagen har landskapet rätt att lagstifta i fråga om utsättande och utdömande av vite samt andra tvångsmedel inom rättsområden som hör till landskapets lagstiftningsbehörighet. Bestämmelser härom kan intas i landskapslagen.

I 45 § finns bestämmelser om administrativ påföljdsavgift. Grundlagsutskottet har av hävd ansett att påföljdsavgifter med avseende på 81 § i grundlagen varken är skatter eller avgifter, utan administrativa påföljder av sanktionskaraktär för en lagstridig gärning. Utskottet har i sak jämställt ekonomiska påföljder av straffkaraktär med straffrättsliga påföljder (GrUU 43/2013 rd). Ålandsdelegationen konstaterar att det ingår i landskapets behörighet att lagstifta om administrativa påföljder med karaktären av sanktioner som ska uppbäras om de skyldigheter som föreskrivs i landskapslagen har försummats i en aktörs verksamhet. Enligt 45 § skulle landskapsregeringen kunna påföra verksamhetsutövare påföljdsavgifter som är betydande. Grundlagsutskottet har påpekat i samband med behandlingen av liknande bestämmelser i rikslagstiftningen att rättssäkerhetsintresset är starkt accentuerat med hänsyn till att påföljdsavgiften är sträng och har karaktär av sanktion. Garantierna för rättssäkerhet och framför allt för behörigt förfarande enligt 21 § i grundlagen och syftena med dem kan anses vara särskilt accentuerade. Att förfarandet för att påföra

påföljdsavgifter är behörigt, oavhängigt och rättvist på det sätt som krävs i 21 § i grundlagen säkerställs genom lagstiftning om att ett kollegialt organ är behörigt att fatta beslut om att påföra påföljdsavgift (se GrUU 14/2018 rd, s. 17–19 och GrUU 24/2018 rd).

I sammanhanget ska även beaktas att bestämmelserna inte verkar utesluta att landskapsregeringen i egenskap av offentlig verksamhetsutövare själv kan vara föremål för påföljdsavgifter. Detta framhåller behovet av ett oavhängigt förfarande för påförande av påföljdsavgifter. Ålandsdelegationen anser att 45 § står i strid med 21 § i grundlagen. Även 46 § bör förordnas att förfalla eftersom paragrafen sammanhänger med 45 §.

Ålandsdelegationen konstaterar att hänvisningen till lagen om rättegång i förvaltningsärenden (FFS 808/2019) i 47 § är förenlig med 25 § i självstyrelselagen om förvaltningsrättsskipningen. Besvär över lagligheten av landskapsregeringens beslut får anföras hos högsta förvaltningsdomstolen.

I landskapslagens 14 § 6 mom., 16 § 3 mom. och 20 § 6 mom. ingår delegeringsbestämmelser. Genom landskapsförordning ska landskapsregeringen kunna utfärda närmare bestämmelser om åtgärder och plan för motståndskraft, formen för och innehållet i incidentrapportering och åtgärder för cybersäkerhet. Enligt 21 § 1 mom. i självstyrelselagen kan landskapsregeringen med stöd av ett bemyndigande i landskapslag utfärda landskapsförordningar i angelägenheter som hör till landskapets behörighet. Genom landskapslag ska dock utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter samt om frågor som enligt grundlagen eller självstyrelselagen i övrigt hör till området för lag. Denna begränsning motsvarar begränsningen i 80 § 1 mom. i grundlagen. Detta innebär att det tydligt ska framgå hur normgivningsmakten delegeras och vilka områden och vilka angelägenheter delegeringen gäller.

Förordningsfullmakterna i 14 § 6 mom. och 20 § 6 mom. möjliggör antagandet av närmare bestämmelser om de åtgärder som riktas till verksamhetsutövare. Vid utfärdandet av förordning får landskapsregeringen inte gå utöver de bestämmelser som avses i 14 § och 20 § och inte heller utfärda förordningar som gäller grunderna för individens rättigheter och skyldigheter eller frågor som enligt grundlagen i övrigt hör till området för lag. Med beaktande av att tillämpningen av bestämmelserna om förordningsfullmakt begränsas av Europeiska unionens lagstiftning anser Ålandsdelegationen att dessa uppfyller förutsättningarna för delegering.

Ålandsdelegationens utlåtande

Med hänvisning till det ovan sagda finner Ålandsdelegationen att hinder för ikraftträdande av landskapslagen inte föreligger, förutom be-

träffande landskapslagens 40 § 1 och 2 mom., 45 § samt 46 §. Landskapslagen torde kunna tillämpas utan de lagrum som föreslås att förordnas att förfalla. Enligt 20 § självstyrelselagen ankommer det på landskapsregeringen att göra en bedömning av situationen, om en landskapslag till en viss del förordnas att förfalla.

Närvarande Ordföranden Holm-Johansson, ledamöterna Dahlén, Leino-Sandberg, Siitari och Åkerblom.

På Ålandsdelegationens vägnar:

Marine Holm-Johansson
ordförande

Sören Silverström
sekreterare