

**Helsingfors/Mariehamn 21.11.2025****Nr 39/25****Hänvisning** Ålands lagtings skrivelse  
26.9.2025, nr 126/2025.

Till Justitieministeriet

**Ärende** Utlåtande över landskapslag om ändring av landskapslagen om cybersäkerhet och motståndskraft, antagen av lagtinget 26.9.2025.**Landskapslagens huvudsakliga innehåll**

Genom landskapslagen ändras landskapslagen (57:2025) om cybersäkerhet och motståndskraft, som trädde i kraft den 1 september 2025. I landskapslagen beaktas sådant som påtalades vid den tidigare lagstiftningskontrollen av landskapslagen om cybersäkerhet och motståndskraft. Ålandsdelegationen gav sitt utlåtande den 26 maj 2025 (ÅD 22/25). Högsta domstolen gav sitt utlåtande den 13 juni 2025 (KKO-HD/442/2025).

Republikens president fann den 27 juni 2025 att något hinder för att landskapslagen träder i kraft inte föreligger, förutom i fråga om 36 § 1 mom. 2 punkten, 38 § 1 mom. 2 punkten, 38 § 2 mom. 8 och 9 punkten, 40 § 1 och 2 mom., 45 § samt 46 §, vilka förordnats att förfalla.

I den föreliggande landskapslagen har införts nya bestämmelser om tillsyns- och efterlevnadsåtgärder, administrativa påföljdsavgifter, en påföljdsavgiftsnämnd, en utvidgad informationsrätt för tillsynsmyndigheten och andra därmed sammanhängande lagtekniska ändringar.

Avsikten är att landskapslagen ska träda i kraft så snart som möjligt.

### Lagstiftningsbehörigheten

Enligt 1 § i den gällande landskapslagen är syftet med landskapslagen att uppnå en hög cybersäkerhetsnivå samt att uppnå en hög grad av motståndskraft och säkerställa tillhandahållandet av samhällsviktiga tjänster. Cybersäkerhet eller något motsvarande begrepp omnämns inte vid fördelningen av lagstiftningsbehörigheten mellan landskapet och riket i självstyrelselagen. Lagstiftningsbehörigheten bör därför bedömas utgående från de rättsområden landskapslagstiftningen berör. Cybersäkerheten är ett område som har likheter och beröringspunkter med informationssäkerhet och även dataskydd. I samband med lagstiftningskontrollen av landskapslagen om cybersäkerhet och motståndskraft var utgångspunkten att den gäller angelägenheter som hör till landskapets lagstiftningskompetens.

Enligt självstyrelselagens 27 § 1 punkt hör stiftande, ändring och upphävande av grundlag samt avvikelse från grundlag till rikets behörighet. Landskapslagens förenlighet med grundlagen bör därför bedömas.

Eftersom det inte tydligt framgick av landskapslagen vad säkerhetsrevisioner gällde eller vilka befogenheter den övervakningsansvarige i fråga hade, ansåg Högsta domstolen med beaktande av 124 § i grundlagen att 36 § 1 mom. 2 punkten, 38 § 1 mom. 2 punkten och 38 § 2 mom. 8 punkten utgjorde en behörighetsöverskridning (se HD 13.6.2025). Eftersom dessa bestämmelser förordnades att förfalla har nya bestämmelser fogats till landskapslagen.

Enligt 36 § 1 mom. 2 punkten kan landskapsregeringen vid tillsyn av en kritisk verksamhetsutövare utföra eller ålägga verksamhetsutövaren att låta utföra säkerhetsrevisioner. Enligt 38 § 1 mom. 2 punkten kan landskapsregeringen vid tillsyn av en väsentlig verksamhetsutövare utföra eller ålägga verksamhetsutövaren att låta utföra regelbundna och riktade säkerhetsrevisioner. Enligt 38 § 2 mom. 8 punkten kan landskapsregeringen vid konstaterade brister eller överträdelser vid efterlevnadskontroll av en väsentlig verksamhetsutövare ålägga verksamhetsutövaren att låta utse en övervakningsansvarig, med väl definierade uppgifter och under en fastställd tidsperiod, i syfte att övervaka verksamhetsutövarens efterlevnad av 20 och 21 §§.

Enligt förarbetena ges landskapsregeringen vidare rätt att själv utföra eller ålägga verksamhetsutövaren att låta utföra säkerhetsrevisioner och att utse övervakningsansvariga. Avsikten har varit att det inte ska ske någon överföring av förvaltningsuppgifter ifrån

tillsynsmyndigheten till det organ vilket utför säkerhetsrevisionen. Det hänvisas också till rikets genomförande i 30 § 1 mom. 1 meningen i cybersäkerhetslagen (FFS 124/2025), vilken granskades av grundlagsutskottet utan anmärkning (se GrUU 62/2024 rd och lagförslag nr 26/2024–2025, s. 5–7).

I grundlagsutskottets praxis har anlitaandet av en revisor eller någon annan utomstående sakkunnig för en utredning som är nödvändig för tillsynen ansetts innebära utförandet av en förvaltningsuppgift. Om bestämmelserna inte ger utomstående självständiga befogenheter utan att det endast handlar om att hjälpa till vid uppdrag finns inget problem med hänsyn till i 124 § grundlagen (GrUU 52/2001 rd, s. 4–5 och GrUU 67/2002 rd).

Landskapslagens 36 § 1 mom. 2 punkt och 38 § 1 mom. 2 punkt utgår från att landskapsregeringen utför säkerhetsrevisionerna. Dock kan landskapsregeringen också ålägga verksamhetsutövaren att utföra uppgiften. Enligt 38 § 2 mom. 8 punkten kan landskapsregeringen ålägga verksamhetsutövaren att låta utse en övervakningsansvarig i syfte att övervaka verksamhetsutövarens efterlevnad av 20 och 21 §§. I förarbetena anges att säkerhetsrevisionerna och övervakningen inte kan innebära direkta rättsföljder för verksamhetsutövaren. Dessa begränsningar i samband med landskapsregeringens ålägganden kunde framgå tydligare ur lagbestämmelserna. Bestämmelser om säkerhetsrevision i cybersäkerhetslagen (FFS 124/2025) var inte föremål för grundlagsutskottets prövning (GrUU 62/2024 rd).

Vid lagstiftningskontrollen förordnades 40 § 1 och 2 mom. om landskapsregeringens rätt att få information av verksamhetsutövarna att förfalla. Bestämmelserna om rätten att få information ansågs vara alltför vag och ospecificerad i ljuset av riksdagens grundlagsutskotts praxis (se ÅD 22/25 och HD 13.6.2025).

I landskapslagens 40 § 1 mom. föreskrivs om mera detaljerade grunder för landskapsregeringens rätt att erhålla information av verksamhetsutövarna. Enligt 40 § 1 mom. 3 punkten har landskapsregeringen trots sekretessbestämmelser och andra begränsningar vilka gäller utlämnande av information följande rätt att få information:

”rätt att av en väsentlig eller viktig verksamhetsutövare få förmedlingsuppgifter, lokaliseringssuppgifter och information om meddelanden vilka innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för tillsynen över fullgörandet av verksamhetsutövarens skyldigheter avseende anmälan och rapportering av betydande incidenter. Den information som landskapsregeringen har fått med stöd av denna punkt är sekretessbelagd.”

Enligt avslutningssatsen till 40 § 1 mom. 3 punkten ska landskapsregeringens rätt till information dock inte begränsa skyddet för vars och ens privatliv, brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden mer än nödvändigt. Ålandsdelegationen konstaterar att avslutningssatsen till 3 punkten inte är lagtekniskt lyckad. I detaljmotiveringen framgår dock att satsen ska tillämpas i förhållande till 1 mom. i sin helhet (lagförslag nr 26/2024–2025, s. 9).

Enligt 10 § 2 mom. i grundlagen är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. Regleringen i grundlagen när det är fråga om förtroliga meddelanden motiveras främst av behovet att skydda innehållet i ett förtroligt meddelande gentemot utomstående.

Grundlagsutskottet har i sitt utlåtande GrUU 62/2024 rd om regeringens proposition (RP 57/2024 rd) till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) konstaterat bl.a. att angående meddelanden som innehåller skadliga datorprogram eller kommando är det inte fråga om kommunikation mellan två parter, utan snarare om verksamhet som allvarligt äventyrar de förtroliga meddelanden som skyddas av 10 § 2 mom. i grundlagen när den orsakar skada för kommunikationsnätets eller informationssystemets funktion. Sådan kommunikation omfattas inte av 10 § 2 mom. i grundlagen, eftersom det saknas ett sådant innehåll som uppkommer mellan fysiska personer som kan betraktas som parter i en kommunikation. Grundlagsutskottet har dessutom noterat att sådana meddelanden som innehåller ett skadligt datorprogram eller kommando helt faller utanför tillämpningsområdet för hemligheten för förtroliga meddelanden i 10 § i grundlagen. Ett sådant meddelande åtnjuter inte skydd enligt 10 § 2 mom. i grundlagen, och bestämmelser om detta behöver inte bedömas utifrån de särskilda eller allmänna förutsättningarna för inskränkning av de grundläggande fri- och rättigheter enligt 10 § 4 mom.

Rätten att få information i 40 § 1 mom. 3 punkten gäller, liksom 28 § 2 mom. i rikets lag, också förmedlingsuppgifter och lokaliseringssuppgifter. Grundlagsutskottet har i sin praxis ansett att behandlingen av lokaliseringssuppgifter anknyter till det skydd för privatlivet som tryggas i 10 § i grundlagen och vars utgångspunkt är individens rätt att leva sitt eget liv utan godtycklig eller ogrundad inblandning av myndigheter eller andra utomstående (t.ex. GrUU 16/2018 rd). Dessutom har bestämmelserna om utredning av lokaliseringssuppgifter samband med den rörelsefrihet som tryggas i 9 § i grundlagen (t.ex. GrUU 16/2018 rd).

I grundlagsutskottets tidigare etablerade praxis har ansetts att identifieringssuppgifterna för ett meddelande ligger utanför kärnområdet för den grundläggande fri- och rättigheten som skyddar

hemligheten i fråga om förtroliga meddelanden (t.ex. GrUU 33/2013 rd). Grundlagsutskottet har dock justerat ovannämnda praxis, eftersom notifieringsuppgifter som anknyter till elektronisk kommunikation samt möjligheten att sammanställa och kombinera dem likväl kan vara problematiska med hänsyn till skyddet för privatlivet på så sätt att en kategorisk uppdelning av skyddet i ett kärnområde och ett randområde inte alltid är motiverad, utan man måste på ett allmännare plan fästa vikt vid hur betydelsefulla begränsningarna är (t.ex. GrUU 18/2014 rd).

Ålandsdelegationen konstaterar att grundlagsutskottet har i sitt utlåtande (GrUU 62/2024 rd) granskat motsvarande bestämmelser som finns i 40 § 1 mom. 3 punkten. Grundlagsutskottet har ansett att den motsvarande regleringen i (28 § 2 mom. i cybersäkerhetslagen) om rätten att få förmedlingsuppgifter är mycket begränsad. Myndigheten har rätt att få information, om det är nödvändigt för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapportering av betydande incidenter. Syftet med rätten att få information har att göra med tryggheten av en störningsfri kommunikation och säkerställandet av kommunikationsnätets funktion och säkerhet. Utskottet har således ansett att regleringen om rätten att få förmedlingsuppgifter i det nu aktuella regleringssammanhanget utgör ett relativt litet ingrepp i skyddet av hemligheten för förtroliga meddelanden, och den måste bedömas utifrån de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheter.

I ljuset av grundlagsutskottets tolkningspraxis framstår avslutningssatsen också som innehållsmässigt vilseledande. Trots att avslutningssatsen är juridiskt problematisk anser Ålandsdelegationen att det inte rör sig om en klar behörighetsöverskridning.

Vid den tidigare lagstiftningskontrollen hänvisades till grundlagsutskottets tolkningspraxis om att rättssäkerhetsintresset i fråga om administrativa påföljdsavgifter är starkt accentuerat med hänsyn till att påföljdsavgiften är sträng och har karaktär av sanktion. Att förfarandet för att påföra sådana påföljdsavgifter är behörigt, oavhängigt och rättvist på det sätt som krävs i 21 § grundlagen säkerställs genom lagstiftning om att ett kollegialt organ är behörigt att fatta beslut om att påföra påföljdsavgift (se GrUU 14/2018 rd). Med beaktande av 21 § i grundlagen och grundlagsutskottets praxis förordnades 45 § i landskapslagen att förfalla. Eftersom 38 § 2 mom. 9 punkten samt 46 § i landskapslagen sammanhängde med 45 § förordnades även dessa lagrum att förfalla.

I 44a § ingår nya bestämmelser om påföljdsavgiftsnämnd som sammanhänger med bestämmelserna om administrativa påföljdsavgifter enligt 45 §. Av 44a § följer att landskapsregeringen

ska utse en till denna ansluten påföljdsavgiftsnämnd, vilken på framställan av landskapsregeringen kan påföra enskilda verksamhetsutövare administrativa påföljdsavgifter. Enligt 38 § 2 mom. 9 punkten kan landskapsregeringen göra en framställning till påföljdsavgiftsnämnden om att verksamhetsutövaren ska påföras en administrativ påföljdssavgift.

Påföljdsavgiftsnämndens funktion och sammansättning är i huvudsak utformad enligt principer som har legat till grund för rikets genomförande i 36 § i cybersäkerhetslagen. Ålandsdelegationen anser att bestämmelserna om påföljdsavgiftsnämnd och administrativa påföljdsavgifter uppfyller de krav som följer av grundlagens 21 § och grundlagsutskottets tolkningspraxis.

Hänvisningen i 46 § till rikslagen om verkställighet av böter (FFS 672/2002) berör rättskipning men kan med stöd av 19 § 3 mom. i självstyrelselagen intas i landskapslagen.

Bestämmelserna om ändringsökande i 47 § 1 och 2 mom. är förenliga med 25 § i självstyrelselagen. Hänvisningen till lagen om rättegång i förvaltningsärenden (FFS 808/2019) kan intas i 47 § 3 mom. med stöd av 19 § 3 mom. i självstyrelselagen.

### **Ålandsdelegationens utlåtande**

Ålandsdelegationen har med beaktande av självstyrelselagens för Åland stadganden funnit att hinder för ikraftträdande av landskapslagen inte föreligger. Ålandsdelegationen har dock ovan i utlåtandet anfört anmärkningar beträffande några stadganden i landskapslagen, men ansett att de inte påverkar behörighetsfördelningen.

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

På Ålandsdelegationens vägnar:

Marine Holm-Johansson  
ordförande

Sören Silverström  
sekreterare