Ålands lagtings beslut om antagande av

Landskapslag om cybersäkerhet och motståndskraft

I enlighet med lagtingets beslut föreskrivs:

1 kap.
Allmänna bestämmelser

1 §
Lagens syfte

Syftet med denna lag är att:

1) uppnå en hög cybersäkerhetsnivå, och

2) uppnå en hög grad av motståndskraft och säkerställa tillhandahållandet av samhällsviktiga tjänster.

2 §
Definitioner

I denna lag avses med:

1) *cybersäkerhetsdirektivet*: Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet),

2) *motståndskraftsdirektivet*: Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG,

3) *den allmänna dataskyddsförordningen*: Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning),

4) *nätverks- och informationssystem*:

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 dirigering 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,

5) *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser vilka kan undergräva tillgängligheten, autenticiteten, riktigheten

eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster vilka erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem,

6) *cybersäkerhet*: cybersäkerhet enligt definitionen i 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 (cybersäkerhetsakten),

7) *tillbud*: en händelse vilken kunde ha undergrävt 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, men vilken framgångsrikt hindrades från att utvecklas eller vilken inte uppstod,

8) *cybersäkerhetsincident*: 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,

9) *storskalig cybersäkerhetsincident*: en cybersäkerhetsincident vilken orsakar störningar vilka är så omfattande att Finland inte kan hantera dem eller vilken har en betydande påverkan på minst två medlemsstater i Europeiska unionen,

10) *incident*: varje händelse vilken kan medföra en betydande störning, eller vilken medför en störning, av tillhandahållandet av en samhällsviktig tjänst, inbegripet när den påverkar de nationella system vilka skyddar rättsstatens principer,

11) *incidenthantering*: alla åtgärder och förfaranden vilka syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident,

12) *risk*: risk för förlust eller störning orsakad av en incident eller cybersäkerhetsincident, vilken ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident eller cybersäkerhetsincident inträffar,

13) *riskbedömning*: den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror vilka skulle kunna leda till en incident och genom att utvärdera den potentiella förlusten eller störningen i samband med tillhandahållandet av en samhällsviktig tjänst till följd av den incidenten,

14) *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i cybersäkerhetsakten,

15) *betydande cyberhot*: ett cyberhot vilket, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande materiell eller immateriell skada,

16) *IKT-produkt*: en IKT-produkt enligt definitionen i artikel 2.12 i cybersäkerhetsakten,

17) *IKT-tjänst*: en IKT-tjänst enligt definitionen i artikel 2.13 i cybersäkerhetsakten,

18) *IKT-process*: en IKT-process enligt definitionen i artikel 2.14 i cybersäkerhetsakten,

19) *sårbarhet*: en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster vilken kan utnyttjas genom ett cyberhot,

20) *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 1025/2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG,

94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (*standardiseringsförordningen*),

21) *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i standardiseringsförordningen,

22) *digital tjänst*: alla informationssamhällets tjänster, det vill säga tjänster vilka vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare,

23) *betrodd tjänst*: en betrodd tjänst enligt definitionen i artikel 3.16 i Europaparlamentets och rådets förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (*förordningen om elektronisk identifiering*),

24) *tillhandahållare av betrodda tjänster*: en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i förordningen om elektronisk identifiering,

25) *kvalificerad betrodd tjänst*: en kvalificerad betrodd tjänst enligt definitionen i artikel 3.17 i förordningen om elektronisk identifiering,

26) *kvalificerad tillhandahållare av betrodda tjänster*: en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i förordningen om elektronisk identifiering,

27) *internetbaserad marknadsplats*: en i 6 kap. 8 § 4 punkten i konsumentskyddslagen (FFS 38/1978) avsedd internetbaserad marknadsplats,

28) *sökmotor*: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (*plattformsförordningen*),

29) *molntjänst*: en digital tjänst vilken möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser,

30) *datacentraltjänst*: en tjänst vilken omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning vilken tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

31) *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

32) *plattform för sociala nätverkstjänster*: en plattform vilken gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer,

33) *företrädare*: en i unionen etablerad fysisk eller juridisk person vilken uttryckligen har utsetts att agera för en leverantör av molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, internetbaserade marknadsplatser, sökmotorer eller en plattform för sociala nätverkstjänster vilken inte är etablerad i unionen, till vilken landskapsregeringen kan vända sig i stället för verksamhetsutövaren, i frågor vilka gäller de skyldigheter som verksamhetsutövaren har enligt denna lag,

34) *allmänt tillgänglig elektronisk kommunikationstjänst*: en tjänst vilken vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och, med undantag för tjänster i form av tillhandahållande av innehåll vilket

har överförts med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller utövande av redaktionellt ansvar över sådant innehåll, omfattar nummeroberoende interpersonella kommunikationstjänster, vilka tillhandahålls till en grupp användare vilken inte har definierats på förhand,

35) *leverantör av utlokaliserade driftstjänster*: en verksamhetsutövare vilken tillhandahåller tjänster vilka rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

36) *leverantör av utlokaliserade säkerhetstjänster*: en leverantör av utlokaliserade driftstjänster vilken utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker,

37) *forskningsorganisation*: en verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men vilken inte inbegriper utbildningsinstitutioner,

38) *motståndskraft*: en kritisk verksamhetsutövares förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident,

39) *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, vilken krävs för tillhandahållandet av en samhällsviktig tjänst,

40) *samhällsviktig tjänst*: en tjänst vilken är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön,

41) *verksamhetsutövare*: en juridisk eller fysisk person, enskild eller offentlig, vilken bedriver verksamhet,

42) *offentlig verksamhetsutövare*: landskapsregeringen och under denna lydande myndigheter och affärsverk, med undantag för Ålands polismyndighet,

43) *nationell strategi för cybersäkerhet*: Finlands nationella strategi för cybersäkerhet enligt 42 § cybersäkerhetslagen (FFS --:--),

44) *nationell strategi för motståndskraft*: Finlands nationella strategi för kritiska aktörers motståndskraft enligt 5 § lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (FFS -:-),

45) *nationell riskbedömning*: Finlands nationella riskbedömning av kritisk infrastruktur och kritiska aktörers motståndskraft enligt 6 § lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft,

46) *NIS-samarbetsgruppen*: samarbetsgruppen vilken inrättas genom artikel 14 i cybersäkerhetsdirektivet,

47) *CSIRT-nätverket*: nätverket för enheter för hantering av cybersäkerhetsincidenter vilket har inrättats genom artikel 15 i cybersäkerhetsdirektivet,

48) *EU-CyCLONe*: det europeiska kontaktnätverket för cyberkriser vilket har inrättats genom artikel 16 i cybersäkerhetsdirektivet,

49) *gruppen för kritiska entiteters motståndskraft*: samarbetsgruppen vilken har inrättas genom artikel 19 i motståndskraftdirektivet,

50) *sakkunnigbedömning*: en sakkunnigbedömning enligt artikel 19 i cybersäkerhetsdirektivet, och

51) *rådgivande uppdrag*: ett rådgivande uppdrag enligt artikel 18 i motståndskraftsdirektivet.

2 kap.
Lagens tillämpningsområde

3 §

Verksamhetsutövare

Denna lag 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 om:

1) verksamhetsutövaren uppfyller eller överstiger definitionen av ett medelstort företag enligt artikel 2 i bilagan till Kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag,

2) verksamhetsutövaren tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst eller en betrodd tjänst,

3) verksamhetsutövaren är den enda leverantören i Finland av en tjänst vilken är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

4) en störning av den tjänst vilken verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa,

5) en störning av den tjänst vilken verksamhetsutövaren tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser,

6) verksamhetsutövaren är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i Finland vilka är beroende av denna verksamhetsutövare,

7) verksamhetsutövaren är en offentlig verksamhetsutövare, eller

8) verksamhetsutövaren har identifierats som en kritisk verksamhetsutövare.

Denna lag ska även tillämpas på verksamhetsutövare om de eller deras verksamheter omfattas av bilagan till motståndskraftsdirektivet och har identifierats som kritiska verksamhetsutövare.

4 §

Avgränsning av tillämpningsområdet

Skyldigheter enligt lagen för verksamhetsutövare att vidta åtgärder för att stärka motståndskraften enligt 4 kap. och åtgärder för cybersäkerhet och rapportering enligt 5 kap., inbegripet sammanhängande bestämmelser om tillsyns- och efterlevnadskontroll i 8 kap., ska inte tillämpas på verksamhetsutövares verksamhet eller tjänster vilka tillhandahålls inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning.

Denna lag tillämpas inte på verksamhetsutövare vilka enbart bedriver sådan verksamhet eller tillhandahåller sådana tjänster vilka avses i 1 mom.

Med avvikelse från 1 och 2 mom. tillämpas lagens skyldigheter för verksamhetsutövare att vidta åtgärder för cybersäkerhet och rapportering enligt 5 kap. alltjämt på verksamhetsutövare vilka är tillhandahållare av betrodda tjänster.

Lagens skyldigheter för verksamhetsutövare att vidta åtgärder för att stärka motståndskraften enligt 4 kap., jämte därmed sammanhängande bestämmelser om internationellt samråd och tillsyns- och efterlevnadskontroll i 8 kap., ska inte tillämpas på kritiska verksamhetsutövare vilka omfattas av sektorn digital infrastruktur i bilagan till motståndskraftsdirektivet.

Lagens bestämmelser vilka förpliktar utlämnande av information ska inte tillämpas om utlämnandet av informationen skulle äventyra försvaret eller

den nationella säkerheten, eller strida mot ett viktigt intresse i samband därmed.

5 §

Förhållandet till annan lagstiftning

Denna lag ska 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.

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.

Den information vilken är sekretessbelagd enligt unionsrättsliga eller andra bestämmelser ska enbart utbytas inom ramen för denna lags skyldigheter med kommissionen och andra berörda myndigheter när ett sådant utbyte är nödvändigt och då begränsas till vad som är relevant och proportionellt för ändamålet med utbytet, med bevarande av informationens konfidentialitet och skyddande av berörda verksamhetsutövares säkerhets- och affärsintressen.

Behandlingen av personuppgifter enligt denna lag ska utföras i enlighet med den allmänna dataskyddsförordningen, landskapslag (2019:9) om dataskydd inom landskaps- och kommunalförvaltningen och landskapslag (2019:74) om tillämpning på Åland av riksförfattningar om dataskydd.

6 §

Jurisdiktion, territorialitet och gränsöverskridande verksamhetsutövare

Denna lag ska tillämpas på verksamhetsutövare vilka är etablerade och bedriver verksamhet eller tillhandahåller tjänster på Åland.

Oberoende av i vilken stat en gränsöverskridande verksamhetsutövare är etablerad ska denna lag tillämpas på de vilka tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst på Åland.

Denna lag ska även tillämpas på gränsöverskridande verksamhetsutövare vilka är leverantörer av molntjänster, datacentraltjänster, nätverk för leverans av innehåll, betrodda tjänster, allmänt tillgängliga elektroniska kommunikationstjänster, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, internetbaserade marknadsplatser, sökmotorer eller plattformar för sociala nätverkstjänster, i den mån de har sitt huvudsakliga etableringsställe på Åland.

En gränsöverskridande verksamhetsutövare ska anses ha sitt huvudsakliga etableringsställe på Åland om det är inom landskapet besluten om åtgärder för cybersäkerhet i huvudsak fattas. Om det inte kan fastställas att besluten om cybersäkerhetsåtgärder fattas inom landskapet eller sådana beslut inte fattas i Europeiska unionen ska det huvudsakliga etableringsstället anses vara beläget på Åland om det är inom landskapet cybersäkerhetsoperationer utförs. Det huvudsakliga etableringsstället ska annars anses vara beläget på Åland om den berörda verksamhetsutövaren på Åland har det etableringsställe vilket har flest anställda inom den Europeiska unionen.

För det fall att en gränsöverskridande verksamhetsutövare inte är etablerad i Europeiska unionen, ska denna lag tillämpas på verksamhetsutövaren om dess utsedda företrädare i Europeiska unionen är

etablerad på Åland. För gränsöverskridande verksamhetsutövare vilka tillhandahåller tjänster på Åland, men inte har utsett en företrädare i Europeiska unionen, tillämpas alltjämt bestämmelserna i denna lag.

Gränsöverskridande verksamhetsutövare vilka omfattas av en annan medlemsstat i Europeiska unionens jurisdiktion men vilka tillhandahåller tjänster eller har ett nätverks- och informationssystem på Åland omfattas 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.

3 kap.
Klassificering, identifiering och informering av verksamhetsutövare

7 §

Kritiska verksamhetsutövare

En verksamhetsutövare vilken omfattas av förteckningen i bilagan till motståndskraftsdirektivet ska av landskapsregeringen, med iakttagande av den nationella riskbedömningen och den nationella strategin för motståndskraft, identifieras som en kritisk verksamhetsutövare om:

1) verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,

2) verksamhetsutövaren bedriver verksamhet och dess kritiska infrastruktur är belägen på Åland, och

3) en incident skulle få betydande störande effekter för verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra verksamhetsutövares samhällsviktiga tjänster, vilka är beroende av den eller de samhällsviktiga tjänsterna.

Vid en bedömning av huruvida en incident skulle få betydande störande effekter enligt 1 mom. 3 punkten ska följande omständigheter beaktas:

1) antalet användare vilka är beroende av den samhällsviktiga tjänst vilken den berörda verksamhetsutövaren tillhandahåller,

2) den grad till vilken andra verksamhetsutövare är beroende av den samhällsviktiga tjänsten i fråga,

3) vilken effekt incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa,

4) verksamhetsutövarens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna,

5) det geografiska område vilket skulle kunna påverkas av en incident, och

6) verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten.

En verksamhetsutövare ska klassificeras som en kritisk verksamhetsutövare av särskild europeisk betydelse om:

1) den av landskapsregeringen har identifierats som en kritisk verksamhetsutövare, och

2) den tillhandahåller samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater i Europeiska unionen och kommissionen på grundval av samråd med landskapsregeringen har fastställt detta samt beslutat att identifiera den som en kritisk verksamhetsutövare av särskild europeisk betydelse.

8 §

Väsentliga verksamhetsutövare

En verksamhetsutövare ska klassificeras som en väsentlig verksamhetsutövare om:

1) verksamhetsutövaren omfattas av förteckningen i bilaga I till cybersäkerhetsdirektivet och överskrider definitionen av ett medelstort företag enligt artikel 2.1 och 3.1–3.3 i bilagan till Kommissionens rekommendation om definitionen av mikroföretag samt små och medelstora företag,

2) verksamhetsutövaren är en tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster och definieras som ett medelstort företag enligt artikel 2 i bilagan till Kommissionens rekommendation om definitionen av mikroföretag samt små och medelstora företag,

3) verksamhetsutövaren är en kvalificerad tillhandahållare av betrodda tjänster,

4) verksamhetsutövaren är en offentlig verksamhetsutövare,

5) verksamhetsutövaren av landskapsregeringen har identifierats som en kritisk verksamhetsutövare, eller

6) verksamhetsutövaren av landskapsregeringen, utifrån kriterierna i 3 § 3–6 punkterna, har identifierats som en väsentlig verksamhetsutövare.

9 §

Viktiga verksamhetsutövare

En verksamhetsutövare vilken omfattas av förteckningarna i bilagorna I eller II till cybersäkerhetsdirektivet samt omfattas av lagens tillämpningsområde och inte har klassificerats som en väsentlig verksamhetsutövare enligt 8 § ska klassificeras som en viktig verksamhetsutövare, inbegripet verksamhetsutövare vilka av landskapsregeringen, utifrån kriterierna i 3 § 3–6 punkterna, har identifierats som viktiga verksamhetsutövare.

10 §

Landskapsregeringens identifiering av verksamhetsutövare och underrättelse

Landskapsregeringen ska senast den 17 juli 2026, samt därefter när så är nödvändigt, identifiera verksamhetsutövare vilka omfattas av förteckningen i bilagan till motståndskraftsdirektivet som kritiska verksamhetsutövare.

Landskapsregeringen ska utan dröjsmål och när så är nödvändigt identifiera andra än redan anmälda klassificerade verksamhetsutövare vilka omfattas av förteckningarna i bilagorna I och II till cybersäkerhetsdirektivet som en väsentlig eller viktig verksamhetsutövare.

Landskapsregeringen ska underrätta de verksamhetsutövare vilka den har identifierat om detta och om deras skyldigheter enligt kapitlen 4 och 5, om det datum från och med vilket dessa skyldigheter är tillämpliga på dem, samt att underrätta kritiska verksamhetsutövare vilka omfattas av sektorn digital infrastruktur i bilagan till motståndskraftsdirektivet om att de inte har några skyldigheter att vidta åtgärder för att stärka motståndskraften enligt kap. 5. Underrättelse ska ske inom en månad från landskapsregeringens informering, med undantag för identifierade kritiska verksamhetsutövare av särskild europeisk betydelse, vilka ska underrättas utan dröjsmål.

11 §

Anmälan av och uppgifter om verksamhetsutövare för förteckning

En verksamhetsutövare vilken har klassificerats som en väsentlig eller viktig verksamhetsutövare ska utan dröjsmål anmäla detta till landskapsregeringen. En verksamhetsutövare vilken har klassificerats eller identifierats som en väsentlig eller viktig verksamhetsutövare ska lämna åtminstone följande uppgifter till landskapsregeringen:

1) verksamhetsutövarens namn.

2) adress och aktuella kontaktuppgifter, inklusive e-postadresser, IP-adresser och telefonnummer,

3) den eller de sektorer och undersektorer enligt förteckningen i bilagorna I eller II i cybersäkerhetsdirektivet som verksamhetsutövaren tillhör, och

4) i tillämpliga fall, en förteckning över de medlemsstater i Europeiska unionen där de tillhandahåller tjänster vilka omfattas av cybersäkerhetsdirektivet.

Leverantörer av molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, internetbaserade marknadsplatser, sökmotorer och plattformar för sociala nätverkstjänster ska utöver uppgifterna i 1 mom. och utan onödigt dröjsmål lämna landskapsregeringen följande uppgifter:

1) den typ av verksamhetsutövare enligt förteckningen i bilagorna I eller II i cybersäkerhetsdirektivet vilken verksamhetsutövaren utgör,

2) adressen till verksamhetsutövarens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i Europeiska unionen eller, om verksamhetsutövaren inte är etablerad i Europeiska unionen, till dess företrädare, och

3) verksamhetsutövarens IP-adressintervall.

En verksamhetsutövare ska utan dröjsmål underrätta landskapsregeringen om ändringar av de uppgifter vilka avses i 1 och 2 mom. denna paragraf. Landskapsregeringen ska underrättas om ändringar av de uppgifter vilka avses i 1 mom. inom två veckor och av de uppgifter vilka avses i 2 mom. inom tre månader från datumet för ändringen.

En verksamhetsutövare vilken har identifierats som en kritisk verksamhetsutövare ska utan dröjsmål underrätta landskapsregeringen om den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater i Europeiska unionen, samt om de samhällsviktiga tjänster vilka den tillhandahåller till eller i dessa medlemsstater och till eller i vilka medlemsstater den tillhandahåller sådana samhällsviktiga tjänster.

12 §

Landskapsregeringens informationsutlämning för förteckning och till kommissionen

Landskapsregeringen ska utan onödigt dröjsmål efter identifiering till ansvarig riksmyndighet överlämna samtliga de uppgifter vilka den behöver för att upprätta en förteckning över kritiska verksamhetsutövare.

Landskapsregeringen ska utan onödigt dröjsmål till ansvarig riksmyndighet överlämna samtliga de uppgifter vilka den behöver för att upprätta en förteckning över väsentliga och viktiga verksamhetsutövare.

Landskapsregeringen ska utan onödigt dröjsmål och därefter vartannat år:

1) underrätta kommissionen och NIS-samarbetsgruppen om antalet väsentliga och viktiga entiteter vilka har förtecknats enligt 2 mom. för varje sektor och undersektor som avses i förteckningen i bilagorna I eller II till cybersäkerhetsdirektivet, och

2) lämna relevant information till kommissionen om antalet väsentliga och viktiga verksamhetsutövare vilka har identifierats av landskapsregeringen, den sektor och undersektor i förteckningen i bilagorna I eller II till cybersäkerhetsdirektivet som de omfattas av, den typ av tjänst vilken de tillhandahåller och de grunder enligt artikel 2.2 b – e i cybersäkerhetsdirektivet, i enlighet med vilka de identifierades.

Landskapsregeringen får även på begäran av kommissionen meddela namnen på de väsentliga och viktiga verksamhetsutövare vilka avses i 3 mom. 2 punkten.

Landskapsregeringen ska utan onödigt dröjsmål underrätta kommissionen om identiteten på identifierade kritiska verksamhetsutövare vilka kan utgöra kritiska verksamhetsutövare av europeisk betydelse samt om den information vilken verksamhetsutövaren har tillhandahållit om dess tillhandahållande av samhällsviktiga tjänster vilken är av betydelse för denna

bedömning. Vid efterföljande samråd med kommissionen ska landskapsregeringen informera kommissionen om den bedömer att de tjänster vilka en kritisk verksamhetsutövare tillhandahåller på Åland utgör samhällsviktiga tjänster.

4 kap.
Kritiska verksamhetsutövares skyldigheter

13 §

Riskbedömning

En kritisk verksamhetsutövare ska inom nio månader från det att den har mottagit en underrättelse om identifiering som kritisk verksamhetsutövare, samt därefter när det är nödvändigt och minst vart fjärde år, på grundval av den nationella riskbedömningen och andra relevanta informationskällor göra en riskbedömning, för att bedöma alla relevanta risker vilka kan störa tillhandahållandet av dess samhällsviktiga tjänster.

En riskbedömning enligt 1 mom. ska innehålla en redogörelse för alla relevanta risker för naturolyckor och risker orsakade av människan vilka skulle kunna leda till en incident, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt övriga hot.

En riskbedömning enligt 1 mom. ska även beakta den grad till vilken andra sektorer i förteckningen i bilagan till motståndskraftsdirektivet är beroende av den samhällsviktiga tjänst vilken tillhandahålls av den kritiska verksamhetsutövaren och den grad till vilken den är beroende av samhällsviktiga tjänster vilka tillhandahålls av andra verksamhetsutövare i sådana andra sektorer, inbegripet i angränsande medlemsstater i Europeiska unionen och, i förekommande fall, tredjeländer.

En kritisk verksamhetsutövare får, om en annan riskbedömning eller ett annat dokument har utarbetats för motsvarande ändamål, använda den bedömningen eller det dokumentet.

Landskapsregeringen kan inom ramen för utövandet av sin tillsynsfunktion slå fast att en annan riskbedömning utförd av en kritisk verksamhetsutövare helt eller delvis uppfyller skyldigheten enligt denna paragraf.

14 §

Åtgärder och plan för motståndskraft

En kritisk verksamhetsutövare ska vidta lämpliga och proportionerliga tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft, på grundval av den nationella riskbedömningen och resultatet av dess egna riskbedömning, inbegripet åtgärder vilka är nödvändiga för att:

1) förhindra incidenter från att uppstå,

2) säkerställa ett tillfredsställande fysiskt skydd av dess lokaler och kritiska infrastruktur,

3) reagera på, stå emot och begränsa konsekvenserna av incidenter,

4) återhämta sig från incidenter,

5) säkerställa en ändamålsenlig hantering av personalsäkerhet, och

6) öka medvetenheten om de åtgärder vilka anges i 1–5 punkterna hos berörd personal.

En kritisk verksamhetsutövare ska i samma syfte utarbeta en plan för motståndskraft, innehållande en beskrivning av de åtgärder vilka har vidtagits enligt 1 mom.

En kritisk verksamhetsutövare får, om en annan plan eller ett annat dokument har utarbetats för motsvarande ändamål, sammanställa motsvarande innehåll i den andra planen eller det andra dokumentet, förutsatt att detta nämns i planen eller dokumentet.

Landskapsregeringen kan inom ramen för utövandet av sin tillsynsfunktion slå fast att en annan plan eller ett annat dokument utarbetat

av en kritisk verksamhetsutövare helt eller delvis uppfyller skyldigheten enligt denna paragraf.

En kritisk verksamhetsutövare ska utse en kontaktpunkt, genom vilken sambandet med landskapsregeringen ordnas.

Landskapsregeringen kan genom landskapsförordning utfärda närmare bestämmelser om åtgärder och plan för motståndskraft enligt 1 och 2 mom.

15 §

Säkerhetsutredning

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.

16 §

Incidentrapportering

En kritisk verksamhetsutövare ska utan onödigt dröjsmål rapportera till landskapsregeringen om incidenter vilka medför en betydande störning eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. En kritisk verksamhetsutövare ska, om det inte är operativt omöjligt, lämna in en första rapport inom 24 timmar efter det att den har fått kännedom om en incident, åtföljd, i förekommande fall, av en detaljerad rapport senast en månad därefter. För att fastställa huruvida störningen är betydande ska i synnerhet följande omständigheter beaktas:

1) antal och andel användare vilka berörs av störningen,

2) störningens varaktighet, och

3) det geografiska område vilket påverkas av störningen.

Incidentrapport enligt 1 mom. ska omfatta all tillgänglig information vilken är nödvändig för att landskapsregeringen ska kunna förstå incidentens art, orsak och möjliga konsekvenser, inbegripet eventuell information vilken krävs för att kunna fastställa incidentens eventuella gränsöverskridande verkningar.

Landskapsregeringen kan genom landskapsförordning utfärda närmare bestämmelser om formen för och innehållet i incidentrapportering enligt 1 och 2 mom.

17 §

Standarder

En kritisk verksamhetsutövare ska sträva efter att i förekommande fall använda tillämpliga europeiska och internationellt erkända standarder och tekniska specifikationer vilka är relevanta för åtgärder för säkerhet och motståndskraft.

18 §

Rådgivande uppdrag

En berörd kritisk verksamhetsutövare av särskild europeisk betydelse ska till ett rådgivande uppdrag ge åtkomst till uppgifter, system och anläggningar vilka rör tillhandahållandet av deras samhällsviktiga tjänster vilka är nödvändiga för utförandet av ett rådgivande uppdrag.

En berörd kritisk verksamhetsutövare av särskild europeisk betydelse ska ta vederbörlig hänsyn till kommissionens yttrande över ett rådgivande uppdrags slutsatser och lämna information till kommissionen och berörda myndigheter i de medlemsstater i Europeiska unionen till eller i vilka den samhällsviktiga tjänsten tillhandahålls om de åtgärder vilka den har vidtagit i enlighet med yttrandet.

5 kap.
Väsentliga och viktiga verksamhetsutövares skyldigheter

19 §

Ledningens styrning och ansvar

En väsentlig eller viktig verksamhetsutövares ledning svarar för verksamhetsutövarens vidtagande av åtgärder för cybersäkerhet och övervakar genomförandet av dem.

Med ledning enligt 1 mom. avses verksamhetsutövarens styrelse, förvaltningsråd och verkställande direktör samt någon annan i därmed jämförbar ställning vilken i praktiken leder dess verksamhet.

En väsentlig eller viktig verksamhetsutövares ledning och dess befattningshavare kan ställas till svars för verksamhetsutövares överträdelser av dess skyldigheter enligt denna lag.

En befattningshavare i en ledning är skyldig att genomgå relevant utbildning och ska uppmuntra verksamhetsutövaren att regelbundet erbjuda liknande utbildning till sina anställda.

20 §

Åtgärder för cybersäkerhet

En väsentlig eller viktig verksamhetsutövare ska vidta lämpliga och proportionerliga tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker vilka hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera cybersäkerhetsincidenters påverkan på användarna av deras tjänster och på andra tjänster.

Åtgärderna enligt 1 mom. ska säkerställa en nivå på säkerheten i nätverks- och informationssystem vilken är lämplig i förhållande till den föreliggande risken. Vid bedömningen av åtgärdernas proportionalitet ska vederbörlig hänsyn tas till verksamhetsutövarens grad av riskexponering, och storlek samt sannolikheten för att cybersäkerhetsincidenter inträffar och deras allvarlighetsgrad.

Åtgärderna enligt 1 mom. ska baseras på en allriskansats syftande till att skydda en verksamhetsutövares nätverks- och informationssystem samt dessa systems fysiska miljö från cybersäkerhetsincidenter och ska åtminstone inbegripa:

1) strategier för riskanalys och informationssystemens säkerhet,

2) incidenthantering,

3) driftskontinuitet och krishantering,

4) säkerhet i leveranskedjan,

5) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,

6) strategier och förfaranden för att bedöma effektiviteten i åtgärderna för cybersäkerhet,

7) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

8) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

9) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och

10) användning inom verksamhetsutövaren, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Övervägande av lämpliga åtgärder enligt 3 mom. 4 punkten ska ske med beaktande de sårbarheter vilka är specifika för varje direktleverantör och tjänsteleverantör, den övergripande kvaliteten på leverantörers och

tjänsteleverantörers produkter och cybersäkerhetspraxis och resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor vilka utförs av NIS-samarbetsgruppen i samarbete med kommissionen och Enisa.

En väsentlig eller viktig verksamhetsutövare vilken finner att den inte följer de åtgärder vilka föreskrivs i 3 mom. ska utan onödigt dröjsmål vidta alla nödvändiga, lämpliga och proportionerliga korrigerande åtgärder.

Landskapsregeringen kan genom landskapsförordning utfärda närmare bestämmelser om åtgärder för cybersäkerhet enligt 1–4 mom.

21 §

Cybersäkerhetsincidentrapportering

En väsentlig eller viktig verksamhetsutövare ska utan onödigt dröjsmål rapportera till landskapsregeringen om alla cybersäkerhetsincidenter vilka har en betydande inverkan på tillhandahållandet av deras tjänster enligt 3 mom. (betydande cybersäkerhetsincidenter). När så är lämpligt ska en berörd verksamhetsutövare utan onödigt dröjsmål underrätta användarna av deras tjänster om betydande cybersäkerhetsincidenter vilka sannolikt inverkar negativt på tjänsternas tillhandahållande. Verksamhetsutövaren ska bland annat rapportera information vilken gör det möjligt för landskapsregeringen att fastställa cybersäkerhetsincidentens eventuella gränsöverskridande verkningar.

Verksamhetsutövaren ska även, i tillämpliga fall, utan onödigt dröjsmål underrätta de användare av deras tjänster vilka kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang vilka dessa användare kan vidta som svar på hotet. När så är lämpligt ska verksamhetsutövaren även informera användare om det betydande cyberhotet.

En cybersäkerhetsincident ska anses vara betydande om:

1) den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för verksamhetsutövaren, eller

2) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Vid rapportering enligt 1 mom. ska verksamhetsutövaren lämna följande till landskapsregeringen:

1) utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande cybersäkerhetsincidenten, en tidig varning vilken i tillämpliga fall ska ange om den betydande cybersäkerhetsincidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar,

2) utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande cybersäkerhetsincidenten, en incidentrapport vilken, i tillämpliga fall, ska uppdatera den information vilken avses i 1 punkten och ange en inledande bedömning av den betydande cybersäkerhetsincidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer,

3) på begäran av landskapsregeringen, en delrapport om relevanta statusuppdateringar,

4) senast en månad efter inlämningen av den incidentrapport vilken avses i 2 punkten, en slutrapport vilken ska innehålla följande:

a) en detaljerad beskrivning av cybersäkerhetsincidenten,

b) den typ av hot eller grundorsak vilken sannolikt har utlöst cybersäkerhetsincidenten,

c) tillämpade och pågående begränsande åtgärder, och

d) i tillämpliga fall, cybersäkerhetsincidentens gränsöverskridande verkningar, och

5) i händelse av en pågående cybersäkerhetsincident vid tidpunkten för inlämnandet av den slutrapport vilken avses i 4 punkten, en lägesrapport vid

den tidpunkten och en slutrapport inom en månad efter det att den har hanterat cybersäkerhetsincidenten.

En verksamhetsutövare vilken är tillhandahållare av betrodda tjänster ska, genom undantag från 4 mom. 2 punkten, när det gäller betydande cybersäkerhetsincidenter vilka påverkar tillhandahållandet av de betrodda tjänsterna, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om en betydande cybersäkerhetsincident, avge en incidentrapport till landskapsregeringen.

Landskapsregeringen kan genom landskapsförordning utfärda närmare bestämmelser om formen för och innehållet i cybersäkerhetsincidentrapportering enligt 1–5 mom.

22 §

Frivillig rapportering

Frivillig rapportering, utöver den rapportering vilken föreskrivs i 21 §, kan avges till landskapsregeringen av:

1) väsentliga och viktiga verksamhetsutövare, avseende på cybersäkerhetsincidenter, cyberhot och tillbud, och

2) andra verksamhetsutövare än de vilka avses i 1 punkten, oberoende av om de omfattas av denna lag, avseende betydande cybersäkerhetsincidenter, cyberhot och tillbud.

23 §

Europeiska ordningar för cybersäkerhetscertifiering

En väsentlig eller viktig verksamhetsutövare ska sträva efter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, vilka har utvecklats av verksamhetsutövaren eller har upphandlats från tredje parter, vilka är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering vilka har antagits i enlighet med artikel 49 i cybersäkerhetsakten.

En väsentlig eller viktig verksamhetsutövare ska sträva efter att använda kvalificerade betrodda tjänster.

24 §

Standarder

En väsentlig eller viktig verksamhetsutövare ska sträva efter att i förekommande fall använda tillämpliga europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i dess nätverks- och informationssystem.

6 kap.
Cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter

25 §

Cyberkrishanteringsmyndighet

Landskapsregeringen är cyberkrishanteringsmyndighet enligt denna lag och ansvarar därmed för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

Landskapsregeringen ska identifiera vilka kapaciteter, tillgångar och förfaranden på Åland som kan nyttjas i händelse av en cybersäkerhetskris.

26 §

Enhet för hantering av cybersäkerhetsincidenter

Landskapsregeringen är enhet för hantering av cybersäkerhetsincidenter enligt denna lag och ansvarar därmed för hanteringen av cybersäkerhetsincidenter på Åland.

Landskapsregeringen ska ha tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med väsentliga och viktiga verksamhetsutövare och andra relevanta intressenter, för vilket ändamål landskapsregeringen bidra till införandet av säkra verktyg för informationsutbyte.

Landskapsregeringen ska samarbeta och, när det är lämpligt, utbyta relevant information om cybersäkerhet med sektoriella eller sektorsövergripande grupper av väsentliga och viktiga verksamhetsutövare.

Landskapsregeringen ska delta i sakkunnigbedömningar.

Landskapsregeringen kan upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter och utbyta relevant information med dem.

Landskapsregeringen kan samarbeta med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter eller motsvarande organ, särskilt i syfte att ge dem cybersäkerhetsstöd.

27 §

Krav på enheten för hantering av cybersäkerhetsincidenter och dess uppgifter

Landskapsregeringen ska, i egenskap av enhet för hantering av cybersäkerhetsincidenter, uppfylla följande krav:

1) landskapsregeringen ska säkerställa en hög nivå av tillgänglighet till sina kommunikationskanaler genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt och den ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa,

2) landskapsregeringens lokaler och de informationssystem vilka den använder sig av ska vara belägna på säkra platser,

3) landskapsregeringen ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar,

4) landskapsregeringen ska säkerställa verksamhetens konfidentialitet och trovärdighet,

5) landskapsregeringen ska ha tillräckligt med personal för att säkerställa att dess tjänster är ständigt tillgängliga och ska säkerställa att personalen har fått lämplig utbildning,

6) landskapsregeringen ska utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i dess tjänster, och

7) landskapsregeringen ska delta i relevanta internationella samarbetsgrupper och nätverk.

Landskapsregeringen ska, i egenskap av enhet för hantering av cybersäkerhetsincidenter, ha följande uppgifter:

1) övervakning och analys av cyberhot, sårbarheter och cybersäkerhetsincidenter på landskapsnivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga verksamhetsutövare avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem,

2) tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga verksamhetsutövare samt till andra relevanta intressenter om cyberhot, sårbarheter och cybersäkerhetsincidenter, om möjligt i nära realtid,

3) vidtagande av åtgärder till följd av cybersäkerhetsincidenter och, i tillämpliga fall, tillhandahållande av stöd till berörda väsentliga och viktiga verksamhetsutövare,

4) insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet,

5) på begäran av en väsentlig eller viktig verksamhetsutövare, tillhandahållande av en proaktiv skanning av verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan,

6) deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med dess kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran, och

7) bidragande till införandet av säkra verktyg för informationsutbyte enligt 25 § 2 mom.

Landskapsregeringen kan utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga verksamhetsutövares allmänt tillgängliga nätverks- och informationssystem, i syfte att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera berörda verksamhetsutövare. Skanningen får dock inte ha någon negativ inverkan på hur en verksamhetsutövares tjänster fungerar.

Landskapsregeringen kan, när den utför de uppgifter vilka avses i 2 mom., prioritera särskilda uppgifter på grundval av en riskbaserad metod.

Landskapsregeringen ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå lagens syfte.

Landskapsregeringen ska, för att underlätta det samarbete vilka avses i 5 mom., främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller förfaranden för incidenthantering, och krishantering.

7 kap.
Landskapsregeringens informationsansvar

28 §

Arrangemang för informationsutbyte

Landskapsregeringen ska underlätta frivilligt informationsutbyte om motståndskraft mellan kritiska verksamhetsutövare, särskilt i fråga om sekretessbelagd och känslig information, konkurrens och skydd av personuppgifter.

Landskapsregeringen ska förenkla rapportering enligt 21 och 22 §§ genom tekniska medel.

Landskapsregeringen ska säkerställa att väsentliga eller viktiga verksamhetsutövare och, i relevanta fall, andra relevanta verksamhetsutövare vilka inte omfattas av denna lags tillämpningsområde, på frivillig basis har möjlighet att utbyta relevant information om cybersäkerhet sinsemellan, om sådant informationsutbyte:

1) syftar till att förebygga, upptäcka, reagera på eller återhämta sig från cybersäkerhetsincidenter eller begränsa deras inverkan, och

2) höjer cybersäkerhetsnivån.

Landskapsregeringen ska säkerställa att informationsutbyte sker inom grupper av väsentliga och viktiga verksamhetsutövare, och i relevanta fall, deras leverantörer eller tjänsteleverantörer, vilket med hänsyn till den potentiellt känsliga karaktären hos den information vilken utbyts ska genomföras med hjälp av arrangemang för informationsutbyte om cybersäkerhet.

Landskapsregeringen ska underlätta inrättandet av de arrangemang för informationsutbyte om cybersäkerhet vilka avses i 4 mom. Landskapsregeringen kan, i samband med fastställandet av närmare bestämmelser om myndigheters deltagande i sådana arrangemang, införa villkor för den information vilken tillgängliggörs av landskapsregeringen. Landskapsregeringen ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med de riktlinjer för att stödja ett frivilligt

informationsutbyte om cybersäkerhet vilka ingår i den nationella strategin för cybersäkerhet.

En verksamhetsutövare ska underrätta landskapsregeringen om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet vilka avses i 3 mom. när de ingår i sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

29 §

Informationsansvar vid incidenter

Landskapsregeringen ska, om en incident hos en kritisk verksamhetsutövare har eller kan ha en betydande påverkan på kontinuiteten i tillhandahållet av samhällsviktiga tjänster i minst sex medlemsstater i Europeiska unionen, anmäla incidenten till kommissionen.

Landskapsregeringen ska genom Finlands gemensamma kontaktpunkt, på grundval av den information vilken en kritisk verksamhetsutövare lämnar i sin incidentrapport, informera gemensamma kontaktpunkter i andra medlemsstater i Europeiska unionen vilka påverkas, om incidenten har eller kan ha en betydande påverkan på kritiska verksamhetsutövare och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i en eller flera andra medlemsstater.

Landskapsregeringen ska, så snart som möjligt efter incidentrapportering enligt 16 §, tillhandahålla berörda kritiskaverksamhetsutövare relevant uppföljningsinformation, inklusive information vilken skulle kunna hjälpa den att reagera ändamålsenligt på incidenten i fråga.

Landskapsregeringen ska informera allmänheten om incidenter om den bedömer att det skulle ligga i allmänhetens intresse.

30 §

Informationsansvar vid cybersäkerhetsincidenter

Landskapsregeringen ska mottaga och hantera rapportering om betydande cybersäkerhetsincidenter enligt 21 § och cybersäkerhetsincidenter, cyberhot och tillbud enligt 22 §.

Landskapsregeringen ska informera Finlands gemensamma kontaktpunkt om de rapporter om cybersäkerhetsincidenter, cyberhot och tillbud vilka inkommer.

Landskapsregeringen ska, utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varning vilken avses i 21 § 4 mom. 1 punkten, lämna ett svar till en rapporterande verksamhetsutövare och om en betydande cybersäkerhetsincident misstänks vara av brottslig art ska vägledning om brottsanmälan tillhandahållas.

Landskapsregeringen kan genom Finlands gemensamma kontaktpunkt vidarebefordra rapporter vilka har mottagits i enlighet med 21 § 1 mom. till de gemensamma kontaktpunkterna i andra berörda medlemsstater i Europeiska unionen.

Landskapsregeringen ska vid en gränsöverskridande eller sektorsövergripande betydande cybersäkerhetsincident se till att Finlands gemensamma kontaktpunkt i god tid förses med relevant information vilken har rapporterats till myndigheten i enlighet med 21 § 4 och 5 mom.

Landskapsregeringen ska, när så är lämpligt, samt särskilt om den betydande cybersäkerhetsincidenten berör två eller flera andra medlemsstater i Europeiska unionen, utan onödigt dröjsmål och genom Finlands gemensamma kontaktpunkt informera enheter för hantering av cybersäkerhetsincidenter i andra medlemsstater och Enisa om en betydande cybersäkerhetsincident. Informationen ska åtminstone inbegripa den vilken har mottagits i enlighet med 21 § 4 mom., med bevarande av verksamhetsutövares säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

Landskapsregeringen kan, om allmänhetens medvetenhet är nödvändig för att förhindra eller hantera en betydande cybersäkerhetsincident, eller om information om en betydande cybersäkerhetsincident på annat sätt ligger i allmänhetens intresse, efter samråd med en berörd verksamhetsutövare, informera allmänheten om en betydande cybersäkerhetsincident eller ålägga den berörda verksamhetsutövaren att göra detta.

Landskapsregeringen ska även behandla frivillig rapportering enligt 22 § i enlighet med de förfaranden vilka anges i 3–7 mom., med givande av företräde åt behandling av obligatorisk rapportering framför frivillig sådan.

Landskapsregeringen ska, vid behov, informera Finlands gemensamma kontaktpunkt om frivillig rapportering vilken har mottagits och samtidigt säkerställa att informationen från rapporterande verksamhetsutövare förblir konfidentiell och skyddas på lämpligt sätt. Utan att det påverkar förebyggande, utredning, avslöjande och lagföring av brott medför inte frivillig rapportering ett ökat ansvar för en rapporterande verksamhetsutövare.

8 kap.
Tillsyn och efterlevnadskontroll

31 §

Tillsynsmyndighet

Landskapsregeringen är tillsynsmyndighet enligt denna lag.

Landskapsregeringen ska agera självständigt och oberoende i sin roll som tillsynsmyndighet.

32 §

Stöd till samt samråd, samarbete och informationsutbyte med verksamhetsutövare om motståndskraft

Landskapsregeringen ska stödja kritiska verksamhetsutövare att stärka deras motståndskraft.

Landskapsregeringen ska samråda, samarbeta och utbyta information och god praxis om motståndskraft med kritiska verksamhetsutövare och relevanta berörda parter.

33 §

Myndighetssamråd och samarbete

Landskapsregeringen ska, när så är lämpligt, samråda och samarbeta om motståndskraft med andra relevanta landskaps- och riksmyndigheter.

Landskapsregeringen ska, när så är lämpligt, samråda om motståndskraft med tillsynsmyndigheter i andra medlemsstater i Europeiska unionen, i syfte att säkerställa att lagstiftningen tillämpas på ett konsekvent sätt och att stärka kritiska verksamhetsutövares motståndskraft samt, om möjligt, minska deras administrativa börda. Sådana samråd ska i synnerhet äga rum avseende kritiska verksamhetsutövare vilka:

1) använder kritisk infrastruktur vilken är fysiskt sammankopplad mellan två eller fler medlemsstater,

2) ingår i företagsstrukturer vilka är sammankopplade eller sammanlänkade med kritiska verksamhetsutövare i andra medlemsstater, eller

3) har identifierats som kritiska verksamhetsutövare i en medlemsstat och tillhandahåller samhällsviktiga tjänster till eller i andra medlemsstater.

Landskapsregeringen ska genom företrädare delta i EU-CyCLONe samt, vid behov med säkerhetsgodkännande, i gruppen för kritiska entiteters motståndskrafts arbete.

Landskapsregeringen ska samarbeta med Finlands gemensamma kontaktpunkt, samordnande cyberskrishanteringsmyndighet, samordnande

enhet för hantering av it-säkerhetsincidenter och tillsynsmyndigheter när det gäller fullgörandet av dessas skyldigheter enligt denna lag och cybersäkerhetslagen.

Landskapsregeringen ska, i syfte att säkerställa att dess uppgifter och skyldigheter om cybersäkerhet utförs på ett effektivt sätt och i den utsträckning det är möjligt samt på ett lämpligt sätt, samarbeta med rikets tillsynsmyndigheter, brottsbekämpande myndigheter, dataskyddsmyndigheter, Transport- och kommunikationsverket och Finansinspektionen jämte andra relevanta tillsynsmyndigheter i landskapet och riket enligt sektorsspecifika unionsrättsakter.

Landskapsregeringen ska regelbundet utbyta information i fråga om cybersäkerhet med Transport- och kommunikationsverket och Finansinspektionen, även när det gäller relevanta cybersäkerhetsincidenter och cyberhot.

Landskapsregeringen ska samarbeta med Finansinspektionen och ska informera det tillsynsforum vilket har inrättats enligt artikel 32.1 i förordningen för digital operativ motståndskraft för finanssektorn när den utövar tillsyns- och efterlevnadskontroll gentemot en väsentlig eller viktig verksamhetsutövare vilken även har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i den förordningen.

Landskapsregeringen ska genom samråd med ansvarig riksmyndighet bidra till framtagandet av Finlands nationella strategier för cybersäkerhet och motståndskraft samt nationella riskbedömning.

34 §

Rådgivande uppdrag

Landskapsregeringen kan begära att kommissionen anordnar ett rådgivande uppdrag för en kritisk verksamhetsutövare, enligt följande:

1) med en berörd verksamhetsutövares samtycke, i syfte att tillhandahålla rådgivning avseende uppfyllandet av dess skyldigheter enligt 4 kap., eller

2) i syfte att bedöma de åtgärder vilka en kritisk verksamhetsutövare av särskild europeisk betydelse belägen på Åland eller vilken tillhandahåller en samhällsviktig tjänst till eller på Åland, har vidtagit.

Landskapsregeringen ska, på begäran från kommissionen, eller av behöriga myndigheter i en eller flera medlemsstater i Europeiska unionen till eller i vilka en kritisk verksamhetsutövare av särskild europeisk betydelses samhällsviktiga tjänst tillhandahålls av en verksamhetsutövare belägen på Åland, tillhandahålla följande information till kommissionen:

1) relevanta delar av verksamhetsutövarens riskbedömning,

2) en förteckning över relevanta åtgärder vilka har vidtagits för att öka verksamhetsutövarens motståndskraft, och

3) de tillsyns- och efterlevnadskontrollåtgärder vilka landskapsregeringen har vidtagit avseende verksamhetsutövaren.

Landskapsregeringen ska analysera den rapport vilken ett rådgivande uppdrag avger över ett uppdrag enligt 1 mom. 2 punkten, ge kommissionen råd om huruvida den berörda verksamhetsutövaren uppfyller sina skyldigheter enligt 4 kap. och, i förekommande fall, vilka åtgärder vilka skulle kunna vidtas för att förbättra verksamhetsutövarens motståndskraft.

Landskapsregeringen ska ta vederbörlig hänsyn till kommissionens yttrande över ett rådgivande uppdrags rapport och lämna information till kommissionen och behöriga myndigheter i de medlemsstater i Europeiska unionen till eller i vilka den samhällsviktiga tjänsten tillhandahålls om åtgärder vilka den har vidtagit i enlighet med yttrandet.

Landskapsregeringen ska, vid samråd med kommissionen och i samband med anordnande av rådgivande uppdrag enligt 1 mom. 2 punkten, föreslå expertkandidater från Åland för deltagande i det rådgivande uppdraget.

Landskapsregeringen ska, för det fall att ett rådgivande uppdrag har ägt rum på Åland, informera gruppen för kritiska entiteters motståndskraft om de viktigaste resultaten av det rådgivande uppdraget och de tillvaratagna erfarenheterna, i syfte att underlätta ett ömsesidigt lärande.

35 §

Sakkunnigbedömning

Landskapsregeringen kan, på grundval av NIS-samarbetsgruppens fastställda metoder, utse cybersäkerhetsexperter för deltagande vid en sakkunnigbedömning.

Landskapsregeringen ska informera kommissionen, Enisa, NIS-samarbetsgruppen och behöriga myndigheter i andra medlemsstater i Europeiska unionen om alla risker för intressekonflikter vilka rör dess utsedda cybersäkerhetsexperter innan en sakkunnigbedömning inleds.

För det fall att Åland är föremål för en sakkunnigbedömning ska följande gälla:

1) landskapsregeringen kan identifiera särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär,

2) landskapsregeringen ska, innan en sakkunnigbedömning inleds informera behöriga myndigheter i deltagande medlemsstater om omfattningen av sakkunnigbedömningen, inbegripet de särskilda frågor vilka har identifierats enligt 1 punkten,

3) landskapsregeringen kan, innan en sakkunnigbedömning inleds, genomföra en självuppskattning av de granskade aspekterna och tillhandahålla den till de utsedda cybersäkerhetsexperterna,

4) landskapsregeringen ska förse utsedda cybersäkerhetsexperter med den information vilken krävs för sakkunnigbedömningen, utan att det påverkar skyddet av sekretessbelagda uppgifter samt skyddet av väsentliga allmänna intressen,

5) landskapsregeringen kan, av vederbörligen motiverade skäl, invända mot utnämningen av en särskild cybersäkerhetsexpert, vilket ska meddelas den andra medlemsstatens utseende behöriga myndighet,

6) landskapsregeringen kan lämna synpunkter på ett utkast till en cybersäkerhetsexperts rapport vilken berör Åland, vilka ska bifogas till rapporten, och

7) landskapsregeringen kan besluta att offentliggöra sin rapport eller en redigerad version av den.

36 §

Tillsyn och efterlevnadskontroll av kritiska verksamhetsutövare

Landskapsregeringen kan vid tillsyn av en kritisk verksamhetsutövare vidta följande tillsynsåtgärder:

1) genomföra inspektioner på plats av kritisk infrastruktur och lokaler, vilka nyttjas för att tillhandahålla en samhällsviktig tjänst, och tillsyn på distans av vidtagna åtgärder för motståndskraft,

2) utföra eller beställa säkerhetsrevisioner, och

3) förelägga verksamhetsutövaren att, inom en rimlig tidsfrist, lämna nödvändig information för att landskapsregeringen ska kunna bedöma vidtagna åtgärder för motståndskraft och bevis på att åtgärderna faktiskt har genomförts.

Landskapsregeringen kan vid konstaterade brister eller överträdelse av skyldigheter enligt 4 kap. vid efterlevnadskontroll av en kritisk verksamhetsutövare, med hänsyn tagen till överträdelsens allvarlighet, förelägga verksamhetsutövaren att, inom en rimlig tidsfrist, vidta nödvändiga och proportionerliga åtgärder för att avhjälpa brister eller överträdelser och att lämna information om vidtagna åtgärder.

37 §

Allmän inriktning på tillsyn och efterlevnadskontroll av väsentliga och viktiga verksamhetsutövare

Landskapsregeringen ska på ett ändamålsenligt sätt övervaka och vidta de tillsyns- och efterlevnadskontrollsåtgärder vilka krävs för att säkerställa att väsentliga och viktiga verksamhetsutövare efterlever denna lag.

Landskapsregeringen kan prioritera tillsyn och fastställa tillsynsmetoder vilka möjliggör att vid utövandet av dess tillsynsuppgifter prioritera uppgifter enligt en riskbaserad bedömning.

Landskapsregeringen ska ha ett nära samarbete med Datainspektionen och Dataombudsmannens byrå när den behandlar cybersäkerhetsincidenter vid väsentliga eller viktiga verksamhetsutövare vilka medför personuppgiftsincidenter.

Landskapsregeringens vidtagna tillsyns- och efterlevnadskontrollåtgärder ska vara effektiva, proportionerliga och avskräckande, med beaktande av omständigheterna i varje enskilt fall. I fråga om efterlevnadskontrollåtgärder ska åtminstone vederbörlig hänsyn tas till följande omständigheter:

1) överträdelsens allvar och betydelsen av de bestämmelser vilka har överträtts, varav följande alltid ska anses utgöra en allvarlig överträdelse:

a) upprepade överträdelser,

b) underlåtenhet att rapportera om eller avhjälpa betydande cybersäkerhetsincidenter,

c) underlåtenhet att avhjälpa brister enligt bindande instruktioner eller föreläggande från landskapsregeringen,

d) förhindrande av revisioner eller övervakningsverksamhet, och

e) tillhandahållande av falsk eller grovt felaktig information,

2) överträdelsens varaktighet,

3) eventuella tidigare relevanta överträdelser,

4) den materiella eller immateriella skada vilken har uppstått, effekter på andra tjänster och det antal användare som berörs,

5) uppsåt eller oaktsamhet,

6) de skadeförebyggande och begränsande åtgärder vilka har vidtagits,

7) efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer, och

8) i vilken utsträckning ansvariga fysiska eller juridiska personer samarbetar med landskapsregeringen.

Landskapsregeringen ska utförligt motivera sina efterlevnadskontrollåtgärder och innan sådana åtgärder vidtas ska landskapsregeringen underrätta den berörda verksamhetsutövaren om dess preliminära slutsatser och bereda den en rimlig tidsfrist för att lämna synpunkter på dessa, förutom i vederbörligen motiverade fall, i vilka omedelbara åtgärder för att förhindra eller reagera på cybersäkerhetsincidenter skulle förhindras.

38 §

Tillsyn och efterlevnadskontroll av väsentliga verksamhetsutövare

Landskapsregeringen kan vid tillsyn av en väsentlig verksamhetsutövare vidta följande tillsynsåtgärder:

1) genomföra inspektioner på plats av lokaler och tillsyn på distans av vidtagna åtgärder för cybersäkerhet,

2) utföra eller beställa regelbundna och riktade säkerhetsrevisioner,

3) utföra ad hoc-revisioner och säkerhetsskanningar, och

4) förelägga verksamhetsutövaren att, inom en rimlig tidsfrist, lämna nödvändig information för att landskapsregeringen ska kunna bedöma vidtagna åtgärder för cybersäkerhet, lämna tillgång till nödvändiga uppgifter,

handlingar och information för att landskapsregeringen ska kunna utföra sina tillsynsuppgifter, och bevis på genomförandet av cybersäkerhetsstrategier.

Landskapsregeringen kan vid konstaterade brister eller överträdelser vid efterlevnadskontroll av en väsentlig verksamhetsutövare vidta följande efterlevnadskontrollåtgärder:

1) utfärda en skriftlig varning till verksamhetsutövaren,

2) anta om bindande instruktioner eller förelägga verksamhetsutövaren att avhjälpa konstaterade brister eller överträdelser,

3) ålägga verksamhetsutövaren att upphöra med handlingssätt vilka utgör en överträdelse och att avstå ifrån att upprepa dessa,

4) ålägga verksamhetsutövaren att säkerställa att nödvändiga åtgärder för cybersäkerhet vidtas eller rapporteringsskyldigheter fullföljs,

5) ålägga verksamhetsutövaren att, inom en rimlig tidsfrist, genomföra de rekommendationer vilka har lämnats till följd av en säkerhetsrevision,

6) ålägga verksamhetsutövaren att informera de fysiska eller juridiska personer vilka potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder vilka dessa kan vidta som svar på hotet,

7) ålägga verksamhetsutövaren att offentliggöra närmare information om dess överträdelser,

8) utse en övervakningsansvarig, med väl definierade uppgifter och under en fastställd tidsperiod, i syfte att övervaka verksamhetsutövarens efterlevnad, och

9) påföra verksamhetsutövaren en administrativ påföljdssavgift.

Landskapsregeringen kan, om efterlevnadskontrollåtgärder enligt 2 mom. 1–5 punkterna är ineffektiva, fastställa en tidsfrist inom vilken verksamhetsutövaren ska ha vidtagit nödvändiga åtgärder för att avhjälpa konstaterade brister eller uppfylla landskapsregeringens krav.

Landskapsregeringen kan, om en enskild väsentlig verksamhetsutövare underlåter att vidta förelagda åtgärder inom en fastställd tidsfrist enligt 3 mom., fram till dess att föreläggandet har efterföljts vidta följande ytterligare efterlevnadskontrollåtgärder:

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.

39 §

Tillsyn och efterlevnadskontroll av viktiga verksamhetsutövare

Landskapsregeringen ska, när den får bevis för, indikationer på eller information om att en viktig verksamhetsutövare underlåter att fullgöra sina skyldigheter enligt denna lag, vid behov vidta tillsyns- och efterlevnadskontrollåtgärder i efterhand.

Landskapsregeringen kan vid tillsyn av en viktig verksamhetsutövare vidta följande tillsynsåtgärder, vidta motsvarande tillsynsåtgärder enligt 38 § 1 mom., med undantag för regelbundna säkerhetsrevisioner och ad hoc-revisioner enligt 2 och 3 punkterna.

Landskapsregeringen kan vid konstaterade brister eller överträdelser vid efterlevnadskontroll av en viktig verksamhetsutövare vidta motsvarande efterlevnadskontrollåtgärder enligt 38 § 2 mom., med undantag för utseende av en övervakningsansvarig enligt 8 punkten.

40 §

Rätt att få information

Landskapsregeringen har trots sekretessbestämmelser och andra begränsningar vilka gäller utlämnande av information rätt att av en verksamhetsutövare få den information vilken är nödvändig för att landskapsregeringen ska kunna utföra sina tillsynsuppgifter och övriga uppgifter enligt denna lag.

Landskapsregeringen ska 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.

Landskapsregeringen har trots sekretessbestämmelser och andra begränsningar rätt att och ska till Finlands gemensamma kontaktpunkter, samordnande cyberskrishanteringsmyndighet, samordnande enhet för hantering av it-säkerhetsincidenter och övriga tillsynsmyndigheter lämna ut den information vilken är nödvändig för att de ska kunna utföra sina uppgifter enligt cybersäkerhetslagen och lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

41 §

Inspektioner

Landskapsregeringen kan utföra inspektioner på plats av kritiska, väsentliga och viktiga verksamhetsutövare inbegripande den kritiska infrastruktur och de lokaler som kritiska verksamhetsutövare använder för att tillhandahålla sina samhällsviktiga tjänster, i syfte att tillse att skyldigheterna enligt denna lag eller beslut fattade med stöd av denna lag fullgörs.

Landskapsregeringen har 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 dock inte ske i utrymmen vilka är avsedda för boende av permanent natur.

Landskapsregeringen har vid inspektion rätt att trots sekretessbestämmelser eller andra begränsningar få redogörelser för och få granska den information och de handlingar, maskinvaror, programvaror, utförda åtgärder och andra säkerhetsarrangemang vilka krävs av verksamhetsutövare enligt denna lag och vilka är nödvändiga för utförandet av tillsynsuppgiften, utförandet av behövliga tester och mätningar samt för att granska de säkerhetsarrangemang vilka verksamhetsutövaren har genomfört.

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. De vilka förrättar inspektionen och vilka deltar i denna ska ha sådan utbildning och erfarenhet vilken behövs för att utföra inspektionen. På utomstående experter tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om skadeståndsansvar återfinns i skadeståndslagen (FFS 412/1974).

På förfarandet vid inspektioner i övrigt tillämpas vad som i 34 § i förvaltningslagen (2008:9) för landskapet Åland föreskrivs om inspektion.

42 §

Internationell handräckning

Landskapsregeringen ska vid tillsyn och efterlevnadskontroll av en gränsöverskridande väsentlig eller viktig verksamhetsutövare vid behov samarbeta med och bistå andra berörda medlemsstaters tillsynsmyndigheter, åtminstone i följande omfattning:

1) landskapsregeringen ska genom Finlands gemensamma kontaktpunkt informera och samråda om de tillsyns- och efterlevnadskontrollåtgärder vilka den har vidtagit,

2) landskapsregeringen kan begära att tillsyns- eller efterlevnadskontrollåtgärder vidtas, och

3) landskapsregeringen ska, efter mottagande av en motiverad begäran därom, tillhandahålla bistånd i form av information eller tillsynsåtgärder.

Landskapsregeringen kan inte avslå en begäran om bistånd enligt 1 mom. 3 punkten vilken riktas till den, med undantag för följande fall:

1) landskapsregeringen saknar behörighet att tillhandahålla det begärda biståndet,

2) det begärda biståndet står inte i proportion till landskapsregeringens tillsynsuppgifter, eller

3) begäran avser information eller innefattar åtgärder som, om den lämnas ut eller de vidtas, skulle strida mot väsentliga nationella säkerhetsintressen, allmän säkerhet eller försvar.

Landskapsregeringen ska, innan den avslår en begäran om bistånd enligt 1 mom. 3 punkten, genom Finlands gemensamma kontaktpunkt samråda med andra berörda tillsynsmyndigheter samt, på begäran av en av dem, även med kommissionen och Enisa.

Landskapsregeringen kan, när så är lämpligt, i samförstånd tillsammans med andra tillsynsmyndigheter vidta gemensamma tillsynsåtgärder.

43 §

Anmälan av överträdelser vilka utgör personuppgiftsincidenter

Landskapsregeringen ska, om den vid tillsyn eller efterlevnadskontroll gentemot väsentlig eller viktig verksamhetsutövare får kännedom om att en överträdelse av skyldigheter enligt 5 kap. även kan utgöra en personuppgiftsincident enligt den allmänna dataskyddsförordningen, utan onödigt dröjsmål anmäla saken till Datainspektionen eller, i tillämpliga fall, Dataombudsmannens byrå.

Landskapsregeringen ska, om den behöriga tillsynsmyndigheten enligt den allmänna dataskyddsförordningen är etablerad i en annan medlemsstat i Europeiska unionen, anmäla saken till Datainspektionen eller, i tillämpliga fall, Dataombudsmannens byrå.

44 §

Vite samt hot om tvångsutförande och avbrytande

Landskapsregeringen kan 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.

45 §

Administrativ påföljdsavgift

Landskapsregeringen kan genom beslut ålägga en enskild verksamhetsutövare, vilken uppsåtligen eller av grov oaktsamhet bryter mot dess skyldigheter enligt denna lag, att erlägga en administrativ påföljdssavgift.

Landskapsregeringen ska i varje enskilt fall, när den fattar beslut om huruvida en väsentlig eller viktig verksamhetsutövare ska påföras en administrativ påföljdsavgift och vid bedömningen av avgiftsbeloppets storlek, ta vederbörlig hänsyn till samma omständigheter enligt 37 § 4 mom. som vid dess vidtagande av övriga efterlevnadskontrollåtgärder.

En administrativ påföljdsavgift vilken påförs en kritisk verksamhetsutövare ska som minst uppgå till 2 000 och som högst till 20 000 euro.

En administrativ påföljdsavgift vilken påförs en väsentlig verksamhetsutövare ska som högst uppgå till 10 000 000 euro eller 2 % av den totala globala årsomsättningen, under det föregående räkenskapsåret, för det företag vilket den väsentliga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

En administrativ påföljdsavgift vilken påförs en viktig verksamhetsutövare ska som högst uppgå till 7 000 000 euro eller 1,4 % av den totala globala årsomsättningen, under det föregående räkenskapsåret, för det företag vilket den viktiga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

Landskapsregeringen ska, om påföljdskollegiet har beslutat att påföra en verksamhetsutövare en administrativ sanktionsavgift enligt den allmänna dataskyddsförordningen, inte påföra en väsentlig eller viktig verksamhetsutövare en administrativ påföljdssavgift för en överträdelse enligt 41 § och vilken följer av samma gärning.

46 §

Verkställighet av påföljdsavgift

Bestämmelser om verkställighet av påföljdsavgifter finns i lagen om verkställighet av böter (FFS 672/2002). En påföljdsavgift preskriberas när fem år har förflutit från den dag då det lagakraftvunna beslutet om avgiften meddelades.

47 §

Ändringssökande

En berörd verksamhetsutövare vilken inte är nöjd med ett av landskapsregeringens beslut får söka ändring genom besvär hos Högsta förvaltningsdomstolen, på det sätt som föreskrivs i lagen om rättegång i förvaltnings-ärenden (FFS 808/2019).

9 kap.
Särskilda bestämmelser

48 §

Ikraftträdande

Denna lag träder i kraft den

Mariehamn den 17 mars 2025

Jörgen Pettersson
talman

Marcus Måtar
vicetalman

Pernilla Söderlund
vicetalman