



Plats: Kommunkansliet i Klemetsby, Lumparland
Tid: Onsdag 6.11.2024 kl. 19.00

ÄRENDEN

143 §	Sammanträdets konstituerande.....	1
144 §	Anmälningssärenden	2
145 §	Kommunfullmäktiges beslut 25.9.2024.....	3
146 §	Inkomstskattesats 2025 (Dnr: 262/2024).....	4
147 §	Fastighetsskattesatser för 2025 (Dnr: 263/2024).....	5
148 §	Klienter inom äldreomsorg placerade i annan kommun (sekretessbelagt enligt 21 § 15 punkten i offentlighetslagen (2021:79) (Dnr: 206/2024).....	6
149 §	Samarbete inom byggnadsinspektion och teknisk förvaltning med Lemlands kommun (Dnr: 225/2024)	10
150 §	Budget 2025 (Dnr: 247/2024).....	14
151 §	Kartläggning av kommunens verksamhet (Dnr: 56/2024)	16
152 §	Avgifter för annonsering i infobladet, kopiering och utlämnande av handlingar (Dnr: 264/2024).....	25
153 §	Avgifter för tillstånd för försäljning av nikotinpreparat samt inspektion (Dnr: 265/2024).....	26
154 §	Bygglovstaxa år 2025 Lumparland (Dnr: 266/2024).....	27
155 §	Barnomsorgstaxa 2025 (Dnr: 226/2024)	29
156 §	Fritidshemstaxa (Dnr: 267/2024)	33
157 §	Äldreomsorgsförvaltningens avgifter (Dnr: 268/2024)	34
158 §	Skolans hyrestaxor (Dnr: 269/2024)	35
159 §	Snöplogningsavgift för privatkunder år 2025, Lumparland (Dnr: 270/2024)	36
160 §	Taxa bilplats med eluttag 2025, Lumparland (Dnr: 271/2024).....	37
161 §	Vattenanslutningsavgift år 2025, Lumparland (Dnr: 272/2024).....	38
162 §	Avloppsanslutningsavgift år 2025, Lumparland (Dnr: 273/2024).....	39
163 §	Avloppsvattentaxa år 2025, Lumparland (Dnr: 274/2024)	40
164 §	Renvattentaxa år 2025, Lumparland (Dnr: 275/2024).....	41
165 §	Lägenhetshyror år 2025, Lumparland (Dnr: 276/2024)	43
166 §	Kapacitetsreservering Lotsbroverket, Lumparland (Dnr: 239/2024).....	45
167 §	Utlåtande VA-plan Åland 2025–2040 (Dnr: 251/2024).....	46
168 §	Marknadsföring av kommunen (Dnr: 188/2023)	47
169 §	Förfrågan om besvär över KEVA:s utjämningsavgifter (Dnr: 277/2024).....	49
170 §	Lagförslag om landskapslag om cybersäkerhet och motståndskraft (Dnr: 256/2024).....	50
171 §	Sammanträdets avslutande	54

Denna sammanträdeskallelse har under tiden 31.10–29.11.2024 anslagits på den elektroniska anslagstavlan för kommunala tillkännagivanden på www.lumparland.ax.
Protokollet publiceras preliminärt 8.11.2024 på kommunens webbsida för protokoll.

Enligt uppdrag:

Kommundirektör

Mattias Jansryd



143 § Sammanträdets konstituerande

Laglighet och beslutförhet

Protokolljustering

Till protokolljusterare utses Göta Alm-Ellingsworth och Eva Jansson.

Protokolljustering sker direkt efter sammanträdets avslutande.

Godkännande av föredragningslistan



144 § Anmälningsärenden

Ks § 144/6.11.2024

1. Tjänsteinnehavarbeslut fattade under kvartal 3:
Kommundirektören
16 § Individuellt tillägg
17 § Utlåtande över ansökan om jordförvärv
18 § Utlåtande över ansökan om jordförvärv
19 § Utlåtande över ansökan om jordförvärv
20 § Anställande av barnskötare
21 § Anställande av närvårdare
22 § Uppsägning av lägenhet
Skolföreståndaren
Överförande av elev till specialpedagogiskt stöd
Äldreomsorgschefen
Beslut om Tillfälligt förordnande: 1
Beslut om socialservice, hemservice/ korttidsvård på serviceboende med heldygnssorg: 2
Beslut om socialservice, trygghetslarm: 2
Beslut om hemserviceavgift: 1
Byråsekreteraren
Beslut om hemvårdsstöds tilläggsdel: 7
Beslut om hemvårdsstöd för syskon: 1
2. Barnomsorgsledarens beslut om utökning av arbetstid för tillfällig barnskötare.
3. Utlåtande från byggnads- och miljönämnden över utkast till Strategi för naturskydd på Åland.
4. Rättelse av beslut gällande landskapsandelar för driften av socialvården och socialtjänsten år 2025, ÅLR.
5. Protokollsutdrag övergripande räddningsplan, ÅLRM.
6. Ägarrapport tertial 2 2024, Åda.
7. Budgetuppföljning och prognos 2024, KST. Helårsprognosen visar en överskridning om 641 00 euro.
8. Med hänvisning till likviditetsstödsansökan har kommundirektören meddelat samtliga enheter att endast nödvändiga inköp får göras fram till kommunen fått besked om ansökan
9. Med hänvisning till likviditetsstödsansökan innehåller kommunen temporärt med vissa betalningar till andra offentliga förvaltningar.

Kommundirektörens förslag

Kommunstyrelsen beslutar anteckna de ovan nämnda ärendena till kännedom.



145 § Kommunfullmäktiges beslut 25.9.2024

Ks § 145/6.11.2024

Enligt 44 § i förvaltningsstadgan ska kommunstyrelsen granska lagligheten av de beslut som fattats av kommunfullmäktige samt tillse att de verkställs.

Följande ärenden behandlades vid kommunfullmäktiges sammanträde 25.9.2024:

- 47 § Samarbete inom byggnadsinspektion och teknisk förvaltning med Lemlands kommun
- 48 § Nytt webbplatspaket
- 49 § Implementering av nytt ekonomisystem

Kommundirektörens förslag

Kommunstyrelsen konstaterar att kommunfullmäktiges beslut är lagliga och att de kan verkställas eller redan har verkställts.



146 § Inkomstskattesats 2025 (Dnr: 262/2024)

Ks § 146/6.11.2024

Budgetförslaget för 2025 utgår från en inkomstskattesats på 19,50 % då kommunstyrelsens budgetdirektiv utgick från den skatteprocenten. Bedömningen är att andra ändringar än i skatteprocenten behöver göras i kommunens finansiering för att på längre sikt få en ekonomi i balans.

Prognosen med nuvarande inkomstskattesats på 19,50 % är att det under 2025 inflyter 1 456 000 euro i inkomstskatt.

Uppskattad påverkan av inkomstskattesatsförändring

1 %	75 000
0,50 %	37 500
0,10 %	7 500

Inkomstskattesatsen ska anges med en tiondels noggrannhet.

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå för fullmäktige att inkomstskattesatsen för 2025 fastställs till 19,50 %.



147 § Fastighetsskattesatser för 2025 (Dnr: 263/2024)

Ks § 147/6.11.2024

Under 2024 har fastighetsskattesatserna varit följande:

Allmän för byggnader	0,60 %
Allmän för markområden	0,60 %
Stadigvarande boende	0,00 %
Övriga bostadsbyggnader	0,90 %
Allmännyttiga samfund	0,00 %
Obebyggd byggplats	1,00 %
Kraftverk	0,60 %

Påverkan av förändring av allmän fastighetsskatt för byggnader

0,10 % 3 000 euro

Påverkan av förändring av allmän fastighetsskatt för markområden

0,10 % 4 000 euro

Påverkan av förändring av fastighetsskatt för stadigvarande boende

0,10 % 8 000 euro

Påverkan av förändring av fastighetsskatt för övriga bostadsbyggnader

0,10 % 4 000 euro

Påverkan av förändring av fastighetsskatt för allmännyttiga samfund

0,10 % 120 euro

Påverkan av förändring av fastighetsskatt för obebyggd byggplats

0,10 % 20 euro

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå för fullmäktige att fastighetskatterna för 2025 fastställs till följande:

Allmän för byggnader	0,60 %
Allmän för markområden	0,60 %
Stadigvarande boende	0,00 %
Övriga bostadsbyggnader	0,90 %
Allmännyttiga samfund	0,00 %
Obebyggd byggplats	1,00 %
Kraftverk	0,60 %



148 § Klienter inom äldreomsorg placerade i annan kommun
(sekretessbelagt enligt 21 § 15 punkten i offentlighetslagen
(2021:79) (Dnr: 206/2024)









149 § Samarbete inom byggnadsinspektion och teknisk förvaltning med Lemlands kommun (Dnr: 225/2024)

Ks § 126/18.9.2024

Lemland och Lumparland har sedan 2012 ett samarbetsavtal för byggnadstekniska sektorn. I maj 2023 valde kommunfullmäktige i Lemland att säga upp samarbetsavtalet, vilket medför att avtalet upphör per den 31.12.2024. Under hösten 2023 har initiala diskussioner förts mellan kommunerna avseende eventuellt framtida samarbete och hur det kan utformas, med en uttalad målsättning om att ha frågan färdigt utredd inom första halvan av 2024.

Under första halvan av 2024 har kommunernas presidier tillsammans med kommundirektörerna diskuterat hur ett framtida samarbete skulle kunna se ut, där Lumparlands kommun haft som målsättning att ta över det drifts- och bokföringsmässiga ansvaret för både byggnadsinspektion och teknisk förvaltning. Ett utkast till samarbetsavtal har tagits fram av förhandlingsgruppen. Utkast till samarbetsavtal, enligt bilaga:

- Bilaga A – Ks § 126

Avtalets innehåll

Tjänsteleverans: Lemlands kommun förbinder sig att leverera tjänster för beredning, beslut och verkställighet inom byggnadsinspektion och kommunal infrastruktur. Detta inkluderar teknisk chef, byggnads- och miljöinspektör samt fastighetsskötare, upp till ett visst antal timmar per vecka.

Beställning: Lumparlands kommun beställer dessa tjänster enligt sitt behov och ansvarar för beslutsfattandet där delegation inte är möjlig.

Ekonomi: Tjänsterna faktureras kvartalsvis utifrån faktiska timmar och enligt en prislista som revideras årligen.

Avtalsperiod: Gäller från 1 januari 2025 med en uppsägningstid på 12 månader.

Det faller således på Lumparlands kommun att ordna beslutsfattandet vad gäller frågor som inte delegerats till tjänsteinnehavare. Således behöver kommunen från 1.1.2025, om avtalet godkänns under hösten, en byggnadsnämnd (lagstadgad) samt ett organ som ansvarar för den tekniska förvaltningen.

Avsikten hos presidiet i förhandlingarna med Lemlands kommun är att den tekniska förvaltningen skulle kunna ligga under kommunstyrelsen då ärendemängden bör vara cirka 2 ärenden per sammanträde, men där tekniska chefen närvarar vid behov. Detta bör minimera det administrativa arbetet för



förvaltningen. Byggnadsnämnd är en lagstadgad nämnd och bygglovshandläggningen kan således inte skötas av kommunstyrelsen. Antalet ärenden som faktiskt behöver ett nämndbeslut enligt nu gällande delegeringsbeslut är dock inte särskilt många per år, men nämnden skulle behöva sammanträde med jämna mellanrum för att ha en jämn handläggning av bygglovsansökningar under året.

Utifrån det beskrivna upplägget håller byggnads- och tekniska kansliet att arbeta med att få fram vilka timmar som uppskattningsvis behöver säljas till Lumparlands kommun och hur mycket som Lemlands kommun själva behöver tjänsteinnehavarna.

Eftersom själva grunden i samarbetsavtalet är överenskommet i förhandlingsgruppen lyfts det nu till kommunstyrelsen och kommunfullmäktige för kännedom.

Kommundirektörens förslag

Kommunstyrelsen tar del av utkastet till samarbetsavtal enligt Bilaga A – Ks § 126 beslutar ge det till kommunfullmäktige för kännedom. Förvaltningen befullmäktigas att arbeta vidare med avtalsutkastet och inkomma med ett slutligt förslag till avtal under hösten.

Beslut

Kommundirektörens förslag godkändes enhälligt.

Kf § 47/25.9.2024

Beslut

Kommunstyrelsens förslag godkändes enhälligt.

Ks § 149/6.11.2024

Ett slutligt avtalsförslag har behandlats i kommunstyrelsen i Lemland vilken föreslår för fullmäktige att godkänna avtalet. Avtalsförslag, enligt bilaga:

- Bilaga B – Ks § 149

Det enda som egentligen är nytt från föregående behandling är att prisbilagan är framtagen. En sammanfattning av prissättningen följer nedan.

Det föreslås att en grundavgift tas ut för de fasta kostnaderna samt en rörlig kostnad som baserar sig på antalet timmar som Lemlands kommun säljer till Lumparlands kommun. Försäljningen har dock begränsats till ett spann för antalet timmar per vecka i medeltal som kan säljas till Lumparlands kommun.



Detta ger en viss flexibilitet, men utan att försäljningen till Lumparlands kommun tillåts bli så omfattande att Lemlands kommun inte kan utföra det egna arbetet enligt plan.

Förslaget är att avtalet löper tillsvidare, med årliga förhandlingar om antalet timmar som kan säljas och med årlig prisjustering. Avtalet föreslås med en ömsesidig uppsägningstid på sex månader, vilket bedöms vara tillräckligt lång tid för att båda kommunerna ska ges en reell möjlighet att ställa om den egna verksamheten.

De timmar som Lemlands kommun erbjuder sig att sälja är följande:

- För kommunal infrastruktur: mellan 11,00 och 21,45 h/vecka i medeltal under ett kalenderår, detta motsvarar mellan 10 och 20 % av den totala veckoarbetstiden för tekniska kansliet.
- För byggnadstillsyn och befolkningskydd: mellan 7,50 och 11,00 h/vecka i medeltal under ett kalenderår, detta motsvarar mellan 12 och 18 % av den totala veckoarbetstiden för byggnadskansliet.
- För skötsel av anläggningar och fastigheter: mellan 38,25 och 40,50 h/vecka i medeltal under ett kalenderår, detta motsvarar mellan 25 och 26,5 % av den totala veckoarbetstiden för fastighetsskötseln.

Lemland och Lumparland kan enligt avtalsförslaget komma överens om tillfällig ökning eller minskning av det antal timmar som säljs. Lemlands kommun förbehåller sig dock rätten att avsäga sig uppdrag som till arbetsmängden enligt Lemlands kommuns bedömning väsentligt överskrider omfattningen av tjänster enligt villkoren i avtalet.

Antalet timmar som avtalet omfattar ska ses över årligen, senast under september månad. Vid dialogen kan parterna komma överens om att försäljningens omfattning antingen ska bibehållas, ökas eller minskas.

Syftet med grundavgiften är att täcka den risk och det ansvar som Lemlands kommun bär samt en andel av de fasta avgifterna som säljaren oundvikligen har. Den löpande timkostnaden är baserad på tre olika sorters tjänster: ledande tjänster och myndighetsutövning, administrativa tjänster samt fastighetsskötsel. Lemlands kommun ska revidera prissättningen årligen, senast den 15 november. Priserna baserar sig på säljarens personalkostnader samt därtill hörande kostnader för utförande av tjänsterna, så som exempelvis nödvändig utrustning och IT-lösningar, och anges exklusive moms.

Avslutningsvis bör nämnas att avtalet ännu inte är behandlat av kommunfullmäktige i Lemland och att eventuella ändringar kan komma att ske i samband med kommunfullmäktiges behandling av ärendet. Preliminärt förväntas kommunfullmäktige i Lemland behandla ärendet 6.11.2024.



Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna avtal om försäljning av tjänster inom kommunal infrastruktur, byggnadstillsyn, befolkningsskydd samt skötsel av anläggningar och fastigheter enligt Bilaga B - Ks § 149. Kommunstyrelsens ordförande och kommundirektören befullmäktigas att slutligt utforma och underteckna avtalet.



150 § Budget 2025 (Dnr: 247/2024)

Ks § 136/15.10.2024

Kommunstyrelsen, kommunfullmäktiges presidium och berörda tjänsteinnehavare håller budgetseminarium i Lumparlands skola inför 2025 års budget. Kommunfullmäktiges ledamöter och kommunstyrelsens ersättare har även bjudits in till seminariet.

Kommundirektörens förslag

Äldreomsorgsförvaltningen, bildningsförvaltningen, tekniska nämnden, byggnads- och miljönämnden, den gemensamma räddningsnämnden, kultur- och fritidsförvaltningen och centralförvaltningen presenterar sina budgetförslag för år 2025 och en allmän diskussion och frågestund hålls i anslutning till detta varefter ärendet remitteras till kommundirektören för vidare beredning.

Beslut

Kommundirektörens förslag godkändes enhälligt.

Ks § 150/6.11.2024

Ett utkast till budget 2025 har tagits fram vilket visar ett underskott på 596 861,80 euro. Budgetförslaget går över den totala ramen kommunstyrelsen gav genom § 102/19.6.2024 med 211 250,88 euro. Årsbidraget budgeteras till 432 043,80. Ramen minskades med 336 258,57 euro i budgetdirektivet för år 2025.

Utkast till budget 2025 och ekonomiplan 2026–27, enligt bilaga:

- Bilaga A – Ks § 150

Anledningarna till ramöverskridningar samt konsekvenser för att försöka landa inom ram har tagits fram, enligt bilaga:

- Bilaga B – Ks § 150

Sammantaget kan konstateras att det är många olika anslag som bidrar till ramöverskridningen inom äldreomsorgsförvaltningen. Lägre inkomster för försäljning av plats till annan kommun samt klientavgifter bidrar till stor del. Att kommunen har en kock anställd vid Kapellhagen förklarar också en stor del av skillnaden gentemot bokslut 2023. Avslutningsvis kostar platser på Sveagården väsentligt mer än i bokslut 2023.



Vad beträffar bildningsförvaltningen är det ökat behov av personal inom barnomsorgen för att möjliggöra för mer administration för daghemsföreståndaren samt skolans plan att gå från två klasser till tre som bidrar till bildningsförvaltningens ramöverskridning.

Kommundirektörens förslag

Kommunstyrelsen tar del av utkastet till budget 2025 och ekonomiplan 2026–27 enligt Bilaga A – Ks § 150 och föreslår eventuella justeringar, varefter den remitteras till kommundirektören, för att återigen behandlas av kommunstyrelsen vid det planerade sammanträdet 27.11.2024.



151 § Kartläggning av kommunens verksamhet (Dnr: 56/2024)

Ks § 30/28.2.2024

I budget 2024 finns ett uppdrag att förvaltningen ska kartlägga kommunens verksamhet för att hitta möjliga effektiviseringar.

Förslag till plan för kartläggning, enligt bilaga:

- Bilaga A – Ks § 30

Det inledande steget i processen innebär en genomgång av kostnader som inte direkt skulle påverka den lagstadgade verksamheten. Därefter följer en kartläggning av kostnader som, även om de inte är direkt lagstadgade, potentiellt kan ha en indirekt inverkan på kommunens lagstadgade verksamhet.

Efter att detta har genomförts kommer hela kommunens personalresurs att granskas noggrant för att säkerställa att den är optimalt dimensionerad. I samband med denna översyn kommer också den praktiska verksamheten att analyseras för att identifiera eventuella arbetsmetoder eller verktyg som kan optimeras för att öka effektiviteten.

Eftersom en betydande del av kommunens IT-infrastruktur är förvaltningsövergripande, kommer en separat analys av IT-miljön och dess struktur att genomföras.

Kommunalförbunden granskas också separat eftersom medlemskap i ett förbund grundar sig i avtal som kommunen inte ensidigt kan ändra.

I det avslutande skedet utförs en noggrann bedömning av vilka av de föreslagna effektiviseringarna som faktiskt är genomförbara. Målet är att presentera ett förslag till förändringar som kan behandlas av kommunstyrelsen och därefter gå vidare till fullmäktige för beslut om genomförande.

Kommundirektörens förslag

Kommunstyrelsen beslutar godkänna planen för kartläggning av kommunens verksamhet enligt Bilaga A – Ks § 30 och överlåter till kommundirektören att tillsammans med kommunens enheter genomföra kartläggningen.

Första delen av kartläggningen där man går igenom icke lagstadgade kostnader, personalresursen och den praktiska verksamheten ska vara klar och kommunstyrelsen tillhanda senast på styrelsesammanträdet i juni.

Beslut

Kommundirektörens förslag godkändes enhälligt.



Ks § 91/19.6.2024

Första delen av kartläggningen är färdigställd. Synpunkter från enheterna, enligt bilaga:

- Bilaga B – Ks § 91

Den praktiska verksamheten

Centralförvaltningen

Centralförvaltningen har en kommundirektör, ekonomichef och byråsekreterare varav de två sistnämnda arbetar på 80 procent.

IT-systemen fungerar, men behov av ett nytt ekonomisystem för att kunna effektivisera verksamheten ses som viktigt, speciellt med tanke på den statistik som ska in till Statskontoret, som nu görs manuellt, samt momsredovisningen. Problemet med nya system verkar tyvärr vara att de är anpassade för mycket större organisationer än Lumparlands kommun och blir då inte så effektiva som man hade hoppats på eftersom att de är för omfattande och även mycket kostsamma.

Vad gäller icke lagstadgade uppgifter rör det sig om administrering av stipendier, administrering av uppvaktningar för personalen och infobladet (skulle kunna göras om till ett digitalt infoblad). Eventuellt skulle kommunen också kunna sluta med arbetstidsredovisning för personal som inte arbetar enligt periodarbete och under förutsättning att man jobbat enligt planerad tid.

Efterarbetet med delgivning, registrering av beslut osv. är relativt tidskrävande. Förtullningen av varor från andra länder än fasta Finland är mycket krångliga och i många fall har man inte möjlighet att göra dem själv för att man inte har tillgång till all information som krävs och blir då tvungen att låta transportbolaget sköta förtullningen vilket innebär att det blir en extra kostnad.

Att vänta in samtliga slutregleringar från kommuner och kommunalförbund till bokslutet är en stor flaskhals som leder till mertid som skulle kunna undvikas om man inte skulle behöva vänta in alla uppgifter som i många fall kommer efter utsatt deadline.

Daghemmet

Daghemmet har en föreståndare/lärare, en lärare, en barnskötare, en resurs samt ett städ-köksbiträde. All personal är kompetent och uppfyller behörighetskraven. Resursen är dessutom överkvalificerad, har lärarutbildning.

Finns behov av visst nytt material samt förnyelse, då inga större inköp gjorts på många år, t ex till daghemsgården. Önskvärt vore att digital utrustning ses över



och kompletteras. Även vissa produkter för barn med NPF (neuropsykiatriska funktionsnedsättningar) skulle behöva köpas in.

Allt arbete som utförs ingår i läroplanen för barnomsorgen på Åland. Barnens behov går naturligtvis i första hand, detta kan innebära att de ibland inte hinner med lagstadgade uppgifter såsom pedagogisk planering och dokumentation, dessa utförs då på övertid/egen tid.

Personal är av åsikten att den pedagogiska dokumentationen är tidskrävande (lärloggar, underlag för specialpedagogiska åtgärder) men det är samtidigt sådant som är nödvändigt och krävs enligt lagen och läroplanen. Den digitala hanteringen kan vara tidskrävande då personalen till viss del saknar kunskaper inom området och då tekniken ofta krånglar.

Brister i datautrustning, ingen uppkoppling till nätet vilket medför att förundervisning, sagostunder och samlingar ibland inte kan genomföras. För föreståndaren kan detta innebära att administrativt arbete inte blir gjort på den planerade tiden, vilket i sin tur gör att hon måste gå från barngruppen på annan tid.

Wilma (ett webbaserat administrationsprogram för närvarohantering och kommunikation mellan hemmet och daghemmet) tar onödigt mycket tid då allt ännu inte är anpassat efter barnomsorgens behov. Som föreståndare måste ännu närvarostatistiken skötas dubbelt, enligt det gamla systemet och i Wilma. Ändringar i vårdtider måste till viss del också göras av föreståndaren.

Fortbildning på området IKT behövs för samtlig personal. Teknologin behöver ses över.

En för kommunen gemensam IKT-ansvarig skulle spara tid och resurser. Vissa inköp kunde göras gemensamt mellan skola och daghem, såsom digital utrustning och andra hjälpmedel. Arbetsbeskrivningarna behöver revideras i enlighet med den nya lagen och läroplanen för barnomsorgen.

Lumparlands skola

För det första kan nämnas att Lumparlands skola fungerar mycket väl och kollegiet bedömer att de har tillräckliga resurser för att sköta de lagstadgade uppgifterna. De gör också bedömningen att de inte utför något frivilligarbete i skolmiljön, utan att de endast sköter det som lagen och läroplanen reglerar.

Lumparlands skola har en årskurs 1–2 och en årskurs 4–6, dvs två klasser. Lumparlands skola har två klasslärare och sedan kompletterar skolföreståndaren med en del undervisning. Skolan har två behöriga lärare och en obehörig som snart är behörig. Därtill finns en elevassistent på cirka 50 procent.



Det skulle i teorin vara möjligt med en enda klass för hela skolans elever, men ur ett pedagogiskt och personalpolitiskt hänseende är det inte att rekommendera.

Biblioteket

Biblioteket sköts av en biblioteksekreterare på 50 procent och öppettiderna är måndagskväll och onsdagskväll samt en timme på onsdag eftermiddag. Av sådant som inte är lagstadgat är det Medis kursplanering och bidragsansökningar. Medis planeringen görs mestadels utanför bibliotekstimmarna. Bidragsansökningarna tar minimalt med tid.

Meröppet kunde gynna låntagare, men detta skulle kräva investeringar i ny teknik och övervakning.

Biblioteket fyller 100 år 2026, så planen är att det borte rummet skulle göras om till barn- och ungdomsbibliotek under 2025, då skolans elevantal förväntas öka igen samma höst. Alla idéer och aktiviteter för att inspirera barnen till mera läsning bör tas till vara.

Äldreomsorgen

Personal på Kapellhagen utgörs av 12 personer varav en av dessa arbetar som kock. All personal är behörig förutom vikariepoolen.

Racer saknas. Tryckavlastande redskap saknas (exempelvis kuddar, madrasser sängar stolar, Comfort rullstol).

Kapellhagen upplever en avsaknad av samarbete med hemsjukvården. Får dock bra hjälp av hemsjukvården Mariehamn, mellan 16:00-08:00.

Vad gäller icke lagstadgade uppgifter hämtar de upp klienter till aktivitet/lunch på Kapellhagen. Kan ta med klient i samband med ärende till stan. Att få följa med på sådan biltur uppskattas mycket av klienterna. Dock genomförs detta i samband med att ett lagstadgat ärende behöver genomföras, vilket således inte låser upp resurser i onödan.

Beträffande flaskhalsar kan nämnas material via hjälpmedelscentralen. Tar lång tid för klienten att få hjälp. Remiss från läkare till att sedan faktiskt få sitt hjälpmedel tar lång tid. Det undermåliga samarbetet från hemsjukvårdens sida kan också nämnas. Klienten ska inte direkt till akuten utan via sjukvårdsupplysningen. Långa telefonköer vilket förhindrar snabb hjälp och rådgivning. Beställningar till ÅHS, behöver beställa långt i förväg för att få i tid. Får ibland sämre ersättningsvaror. Åhs tar inte tillbaka. Dialog förs inte innan sämre varor skickas ut. Betalar fullt pris för varorna som kommit trots att det är ersättningsvaror.

Samarbetet på Kapellhagen upplevs fungera bra. Det finns en befintlig struktur som fungerar. Alla vet vad som ingår i respektive pass. Viss frihet finns inom



kompetens/behörighet. Kunna göra adekvata bedömningar gällande de äldres hälsotillstånd ingår i behörigheten. Avslutningsvis bör Kapellhagen se över rutinerna gällande medicinering.

Byggnadstekniska sektorn

Samarbetsavtalet inom byggnadstekniska sektorn är under förhandling. Som det ser ut nu kommer Lumparlands kommun att överta driften av byggnadstekniska sektorn. Det är först då som kommunen kan se i detalj hur den sektorn arbetar. Exempelvis skulle en översyn av kommunens hyresbostadsbestånd vara lämpligt att utföra.

Brand- och räddning

Kommunen har nyligen godkänt en för Åland gemensam räddningsmyndighet som startade upp i maj 2024. Det återstår att se vilka stordriftsfördelar som kan komma av den.

Icke lagstadgade kostnader

Kartläggning av icke lagstadgade kostnader, enligt bilaga:

- Bilaga C – Ks § 91

Centralförvaltningen

Här är det främst småsummor. De största posterna är arvoden och medlemskap i kommunförbundet. Friskvården kostar en del men kan inte anses vara något som ska dras in.

Daghemmet

Daghemmet har endast mindre summor. De har också nämnt i sin kartläggning att anslagen för inköp till verksamheten borde vara något högre för att kunna byta ut saker. Det skulle eventuellt vara möjligt att föra över barnomsorgsledning på daghemsföreståndare och kommundirektör, men det förutsätter mer administrationstid för daghemsföreståndaren.

Skolan

Skolskjutsarna är förvisso lagstadgade och gick också under budget i senaste upphandlingen, men är fortfarande en stor post. Livsmedel är förstås inget som kan tas bort men det går att få ner kostnader genom att handla billigare. I övrigt är det bara mindre summor.

Biblioteket/kultur- och fritid

Det går att skära i litteraturbudgeten, men den är redan skuren i för några år sedan. Ungdomsgården går att stänga ner då det inte är lagstadgad verksamhet. Alla bidrag till föreningar går också att dra in. Samlingslokalstödet till Furuborg är också fullt möjligt att avsluta. Det finns heller inget krav på att vara med i Medis.



Äldreomsorgen

Det går även här att få ner kostnaderna för livsmedel om man handlar billigare. I övrigt är det bara små anslag.

Kommundirektörens förslag

Kommunstyrelsen beslutar vilka delar, om några, av kartläggningen som föranleder närmare utredningar som skulle kunna möjliggöra för effektiviseringar.

Beslut

Kommunstyrelsen beslöt enhälligt att varje förvaltning bör inkomma med tre konkreta förslag till förbättringar, resursförändringar och/eller förvaltningsöverskridande samarbeten. Styrelsen emotser svar senast 6.9.2024 och avser ha ett gemensamt forum där de olika förslagen diskuteras, som preliminärt ordnas 12.9.2024.

Ks § 125/18.9.2024

Inför kommunstyrelsen forum med enheterna 12.9.2024 lämnades följande förslag in, enligt bilaga:

- Bilaga D – Ks § 125

Under diskussionerna framkom följande som uppfattades som särskilt intressant:

- Samplanering genom en så kallad centralköksfunktion
- Hålla biblioteket stängt under bibliotekssekreterarens semester, förutom sommaren
- IKT-ansvarig i SÅUD även för daghemmen
- IKT-ansvarig i kommunen med en särskild ersättning
- En för alla enheter gemensam upphandling av kontorsmaterial
- Större samplanering av semestrar mellan skolans och Kapellhagens kök nu när det finns kock på båda enheterna
- Kontinuerligt utbytande av idéer kvartalsvis mellan enheter inom exempelvis dataprogram

Kontentan av forumet är att det är mycket svårt att hinna några större inbesparingar eftersom så mycket av verksamheten är lagstadgad och personaltung, men mindre effektivisering bör vara möjligt, speciellt inom livsmedel och kök.

Parallellt med kommunens egna kartläggning genomförs mellan storleksmässigt likvärdiga kommuner en jämförelse utifrån en rad olika



nyckeltal för att se var man eventuellt sticker ut kostnadsmässigt. Den bör bli klar under oktober månad.

Kommundirektörens förslag

Kommunstyrelsen beslutar att förvaltningen går vidare med att utreda följande:

- Samplanering genom en så kallad centralköksfunktion samt samplanering av semestrar under sommaren
- En för alla enheter gemensam upphandling av kontors- och förbrukningsmaterial
- Fråga SÅUD om eventuell IKT-ansvarig gentemot distriktets daghem
- Särskild ersättning för en IKT-ansvarig kommunen
- Hålla biblioteket stängt under bibliotekssekreterarens semester, förutom sommaren
- Konkretisera utbytet av idéer och erfarenheter mellan enheterna

Beslut

Kommundirektörens förslag godkändes enhälligt.

Ks § 151/6.11.2024

Som utlovades vid förra behandlingen av ärendet har en jämförelse med storleksmässigt likvärdiga kommuner gjorts utifrån en rad olika nyckeltal för att se var man eventuellt sticker ut kostnadsmässigt. Det kan dock nämnas att inte alla kommuner fullständigt fyllt i sina uppgifter och att det fortsättningsvis är ett arbetsdokument. Jämförelse, enligt bilaga:

- Bilaga E – Ks § 151

Som framgår av jämförelsen sticker inte Lumparlands kommun ut kostnadsmässigt med undantag för kostnaden per elev.

Dock är kommunens totala kostnad för skolan inget som fordrar uppmärksamhet. Det är egentligen ingen kommun som har anmärkningsvärda kostnader som föranleder någon oro för kostnadsineffektivitet. Jämförelsen torde visa att kommunerna driver sina förvaltningar till en kostnad som motsvarar de lagkrav kommunerna har på sig, eller åtminstone att samtliga kommuner bedriver service på ett likvärdigt sätt. Av de jämförda kommunerna är det tre kommuner som inte sedan 2020 har gjort ett överskott i sina resultat, vilka är Föglö, Kumlinge och Lumparland. Dessa kommuner ser inte heller ut att göra något positivt resultat 2024 och budgeterar också ett negativt resultat 2025.

Av jämförelsen kan man dra några slutsatser. För det första så gör Lumparlands kommuns invånares relativt höga skattekraft att kommunen inte får någon



större skattekomplettering, utan landskapsandelssystemet antar att våra kommuninvånare klarar att upprätthålla lagstadgad service med en relativt liten skattekomplettering. Jämför detta med Geta som på grund av sin låga skattekraft får en mycket hög skattekomplettering genom systemet.

Lumparlands kommun räknas inte som en skärgårdskommun enligt landskapsandelssystemet, medan Vårdö kommun gör det. Vårdö kommun får bland annat på grund av det en landskapsandel som är cirka 1 500 euro mer per invånare än Lumparlands kommun. Skatteinkomsterna totalt är dock relativt lika som Lumparland. Om Lumparlands kommun skulle få en landskapsandel som motsvarar Vårdö kommun skulle Lumparland ha en landskapsandel på 1 303 924 euro, vilket skulle medfört att kommunen hade gjort ett positivt resultat om cirka 250 000 euro 2023. Nu är det förstas inte så enkelt eftersom det finns en rad olika parametrar i landskapsandelssystemet som styr ersättningen, men kontentan av jämförelsen mellan kommunernas driftskostnader och kommunernas skatter och landskapsandelar är att vissa kommuner inte drar fördel som helhet av systemets parametrar medan andra kommuner som helhet gör det.

Lumparlands kommun kan inte, utifrån jämförelsen med andra kommuner, anses drivas kostnadsineffektivt utan helt i paritet med andra perifera kommuner. Det som emellertid kan nämnas är att utifrån verksamhetsbidrag/invånare så förefaller Geta kommun vara den mest effektiva av de mindre kommunerna. Detta får en att dra slutsatsen att Lumparlands befolkningsmängd i relation till den service befolkningen har lagstadgad rätt till inte räcker till för att upprätthålla den med nuvarande landskapsandelar, medan Geta med cirka 150 fler invånare och landskapsandel om cirka 1 000 euro mer per invånare än Lumparland ges förutsättningar att hålla sig flytande på ett bättre sätt, även om Geta antagligen kan klassas som en kriskommun enligt föreslagen lagstiftning.

Slutsatsen av den är kortare analysen är att Lumparlands kommun behöver en av två saker:

- En större befolkningsmängd som fortsättningsvis har en stark skattekraft.
- En landskapsandel som motsvarar vad en vissa andra perifera kommuner erhåller.

Den förstnämnda är inget som görs i en handvändning utan något som görs över 10-tals år. Den sistnämnda är helt beroende av politik. Det sistnämnda alternativet är görbart på kort tid i teorin, men med tanke på den fatala haveri i i landskapspolitiken vad gäller landskapsandelarna, som stått stilla sedan 2009 bör inte Lumparlands kommun sätta något förtroende för att landskapsregeringen tillsammans med lagtinget lyckas skapa en långsiktigt hållbar finansiering av kommunerna, utan kommer högst antagligen att driva



merparten av Ålands kommuner till ruinens brant eller längre innan någon långsiktig lösning tas fram. Den totala landskapsandelen var 41 749 000 euro 2009 och var 42 954 000 euro år 2023. I 2023 års belopp är kompensation för grundavdrag och reseavdrag inräknat, vilket inte i egentlig mening är en landskapsandel utan ersättning för förlorade skatteinkomster. Landskapsandelen i medeltal från 2009 till 2023 har varit 37 948 000 euro. Således har kommunerna efter 2009 fått mindre i landskapsandelar per år i medeltal. Här kan nämnas att kommunernas verksamhetsbidrag (kostnader efter intäkter) har ökat med cirka 57 000 000 euro eller 55 procent. Om Lumparlands kommun skulle få en landskapsandel som motsvarar en procentuell andel av verksamhetsbidraget i paritet med 2009 skulle kommunen under 2023 erhållit en landskapsandel på 1 214 000 euro.

Med anledning av vad som framkommer ovan har ett förslag till skrivelse tagits fram. Säkerligen är det som framkommer ovan eller i skrivelsen inte någonting nytt, men det tål att poängteras att den ekonomiska situation som kommunerna står inför inte är förorsakat av kommunerna eller dess invånare, utan en fallerad ekonomisk politik på landskapsnivå gentemot kommunerna.

Skrivelse, enligt bilaga:

- Bilaga F – Ks § 151 (kompletteras innan sammanträdet)

Kommundirektörens förslag

Kommunstyrelsen beslutar översända skrivelsen enligt Bilaga F – Ks § 151 till Ålands landskapsregering och Ålands lagting och delger ärendet i sin helhet till kommunfullmäktige och föreslår samtidigt att fullmäktige konstaterar uppdraget i budget 2024 att kartlägga kommunens verksamhet slutfört.



152 § Avgifter för annonsering i infobladet, kopiering och utlämnande av handlingar (Dnr: 264/2024)

Ks § 152/6.11.2024

Lumparlands kommun tar ut avgifter för annonsering i infobladet och för att ta fotokopior på kommunkansliet. Förslag till avgifter för annonsering i Infobladet och kopiering och utlämnande av handlingar, enligt bilaga:

- Bilaga A – Ks § 152

Privatpersoner bosatta i Lumparland får avgiftsfritt införa en annons på 1/4 sida per infoblad.

Föreningar i Lumparland får avgiftsfritt införa en annons på 1/1 sida per infoblad.

Kommunalförbund i vilka Lumparlands kommun är medlem och kommuner med vilka Lumparlands kommun har samarbetsavtal får avgiftsfritt införa annonser i infobladet.

Allmännyttiga samfund i Lumparland kopierar svartvita kopior avgiftsfritt.

Följande ändringar föreslås:

- 1/1 sida höjs från 28 euro till 30 euro
- ½ sida höjs till från 17 euro till 20 euro
- ¼ sida höjs från 12 euro till 15 euro
- Prenumeration på infobladet per år höjs från 28 euro till 50 euro
- Alla kopior och utskrifter höjs med 0,20 cent

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna avgifter för annonsering i infobladet, kopiering och utlämnande av handlingar enligt Bilaga A – Ks § 152 att gälla från och med 1.1.2025.



153 § Avgifter för tillstånd för försäljning av nikotinpreparat samt inspektion (Dnr: 265/2024)

Ks § 153/6.11.2024

Försäljning av nikotinpreparat på andra ställen än apotek förutsätter ett detaljhandelstillstånd för nikotinpreparat. Tillståndet ansöks vid den kommun som försäljningsplatsen ligger i. Sedan 2022 är det avgiftsbelagt i kommunen att beviljas tillstånd för försäljningen samt för tillståndet förutsatt inspektion över försäljningsstället.

Förslag till avgifter, enligt bilaga:

- Bilaga A – Ks § 153

Avgifterna föreslås höjas med 2 procent, avrundat till närmsta heltal.

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna avgifter för tillstånd för försäljning av nikotinpreparat samt inspektion enligt Bilaga A – Ks § 153 att gälla från 1.1.2025.



154 § Bygglovstaxa år 2025 Lumparland (Dnr: 266/2024)

Bmn § 91/16.9.2024

I nuläget har inkommit 12 bygglovsärenden i Lumparland under år 2024. Våningsytan är 250 m².

I fjol var bygglovsärendena vid denna tidpunkt 23 och våningsytan 1650 m².

Enligt PBL 99 § är den som söker bygglov, annat tillstånd eller gör en anmälan skyldig att betala en avgift till kommunen enligt en taxa som fastställts av kommunfullmäktige.

Dessa avgifter är ersättning för myndighetsuppgifter och därför momsbefriade.

Bygglovstaxan för byggnadstillsyn och dylikt för Lumparland år 2025 ska fastställas av fullmäktige i Lumparland.

Lite ekonomisk statistik

BS 2021 kostnadstäckning 44 %
BS 2022 kostnadstäckning 29 %
BS 2023 kostnadstäckning 46 %
BU 2024 kostnadstäckning 36 %

Genom att det för tillfället söks färre bygglov för större byggnader än tidigare ligger inkomstnivån på en lägre nivå än tidigare.

Bygglovstaxan har höjts med 2 % från 2024 års nivå, undantaget taxorna för brandsyner som stiger ca 20 % p g a räddningsmyndighetens nya prissättning av sina tjänster.

Byggnads- och miljöinspektörens förslag

Nämnden besluter omfatta förslaget till bygglovstaxa för Lumparland år 2025. Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Beslut

Nämnden omfattade byggnads- och miljöinspektörens beslutsförslag.

Bilagor

Bygglovstaxa 2024 Lumparland

Bygglovstaxa 2025 Lumparland



Ks § 154/6.11.2024

Förslag till bygglovstaxa, enligt bilaga:

- Bilaga A – Ks § 154

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna bygglovstaxan enligt Bilaga A – Ks § 154 att gälla från och med 1.1.2025.



155 § Barnomsorgstaxa 2025 (Dnr: 226/2024)

Ks § 130/18.9.2024

Barnomsorgsledarens beredning

Enligt landskapslagen om ändring av landskapslagen om barnomsorg och grundskola (ÅFS 2022:55) § 22 mom. 4 ska kommunen senast tre månader före en ändring av avgifterna införs meddela om ändringar, det vill säga den 30 september 2024.

Kommunen har i nuläget tre olika avgiftskategorier enligt nuvarande lagstiftning; Heltid (100 %), deltid (80 %), halvtid (60 %). Det föreslås ingen förändring av taxorna då kommunen i dagsläget uppbär de maxavgifter som är fastslagna i gällande lagstiftning.

Enligt LL om barnomsorg och grundskola del II 14 § mom. f) beviljas barnomsorg i daghemsverksamhet i den utsträckning det är förenligt med barnets bästa. Endast i särskilda fall kan det anses förenligt med barnets bästa att vistas i barnomsorg i daghemsverksamhet längre än 10 timmar per dygn eller längre än 200 timmar per månad.

Tolkningen inom SÅUD är att eftersom det står 200 timmar per månad så är 200 timmar det maximala antalet som vårdnadshavare ska kunna boka. Om det är som nu 10 timmar/dag som skall kunna bokas så är det onödigt att det står 200 timmar per månad eftersom det inte kommer att räcka till de månader som har fler än 20 verksamhetsdagar.

För att kunna få vårdtidsbokningen i Wilma att fungera så är det nödvändigt att antalet tillgängliga timmar är de samma under varje månad för de olika vårdkategorierna.

Därav föreslås det att heltidsbarnomsorg utgör 200 timmar/månad. Därav följer även tolkningen att deltidbarnomsorg utgör 160 timmar/månad och halvtidsbarnomsorg utgör 120 timmar/månad.

Förundervisningen är, enligt gällande lagstiftning, avgiftsfri sedan 1.1.2021 och skall vara minst 4 h/dag. I Lumparland är förundervisningen 4 h/verksamhetsdag. Lemland har tillämpat att förundervisningen är 5 h/verksamhetsdag, motsvarande en deltidsp plats. Även syskonrabatten är olika i kommunerna, Lumparland har en fast avgift medan Lemland har procent.



Lumparland:

- 25 euro per barn för heltidsplats
- 20 euro per barn för deltidspäls
- 15 euro per barn för halvtidspäls
- 10 euro per barn för fritidshem

Lemland:

- 0 % för barn 1
- 10 % för barn 2
- 30% för barn 3, barn 4 osv.

För att få det lika i kommunerna och även underlätta det administrativa arbetet föreslås det att Lumparland inför förundervisning 5h/ verksamhetsdag samt att syskonrabatten ändras så att den blir lika som i Lemland.

Förslag till barnomsorgstaxa och avgiftstillämpning, enligt bilaga:

- Bilaga A – Ks § 130

Utbildningschefen förordar

Kommunstyrelsen beslutar att barnomsorgsavgifterna och avgiftstillämpningen från och med 1.1.2025 för kommunens daghem fastställs enligt Bilaga A – Ks § 130.

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att barnomsorgsavgifterna och avgiftstillämpningen från och med 1.1.2025 för kommunens daghem fastställs enligt Bilaga A – Ks § 130.

Beslut

Kommunstyrelsen beslöt enhälligt återremittera ärendet.

Ks § 155/6.11.2024

Barnomsorgsledarens beredning

Enligt LL om barnomsorg och grundskola (ÅFS 2020:32) ska kommunen senast tre månader före en ändring av avgifterna införas meddela om ändringar, det vill säga den 30 september 2024. Enligt landskapslagen om ändring om landskapslagen om barnomsorg och grundskola (ÅFS 2022:50) kan kommunen meddela om sådana ändringar av avgifterna följer denna lag senast en månad före ändringarna införas.

Kommunen har i nuläget tre olika avgiftskategorier enligt nuvarande lagstiftning; Heltid (100 %), deltid (80 %), halvtid (60 %). Det föreslås ingen



förändring av taxorna då kommunen i dagsläget uppbär de maxavgifter som är fastslagna i gällande lagstiftning.

Enligt LL om barnomsorg och grundskola del II 14 § mom. f) beviljas barnomsorg i daghemsverksamhet i den utsträckning det är förenligt med barnets bästa. Endast i särskilda fall kan det anses förenligt med barnets bästa att vistas i barnomsorg i daghemsverksamhet längre än 10 timmar per dygn eller längre än 200 timmar per månad.

Tolkningen inom SÅUD är att eftersom det står 200 timmar per månad så är 200 timmar det maximala antalet som vårdnadshavare skall kunna boka. Om det är som nu 10 timmar/ dag som skall kunna bokas så är det onödigt att det står 200 timmar per månad eftersom det inte kommer att räcka till de månader som har fler än 20 verksamhetsdagar.

För att kunna få vårtdidsbokningen i Wilma att fungera så är det nödvändigt att antalet tillgängliga timmar är de samma under varje månad för de olika vårdkategorierna.

Därav föreslås det att heltidsbarnomsorg utgör 200 timmar/månad. Därav följer även tolkningen att deltidbarnomsorg utgör 160 timmar/månad och halvtidbarnomsorg utgör 120 timmar/månad.

Förundervisningen är, enligt gällande lagstiftning, avgiftsfri sedan 1.1.2021 och skall vara minst 4 h / dag. I Lumparland är förundervisningen 4 h/verksamhetsdag. Lemland samt Jomala och Hammarland i distriktet har tillämpat att förundervisningen är 5 h/ verksamhetsdag, motsvarande en deltidsp plats. För att få en likvärdig barnomsorg i distriktet är det önskvärt att Lumparland inför förundervisning 5h/verksamhetsdag. Nämnas kan att när vårdnadshavare/ familjer funderar på att flytta till kommuner så jämför de ofta bl.a hur barnomsorgen ordnas och förundervisningen en av de delar som jämförs.

För att få det lika i kommunerna och även underlätta det administrativa arbetet föreslås det att Lumparland inför förundervisning 5h/ verksamhetsdag.

Nytt förslag till barnomsorgstaxa och avgiftstillämpning, enligt bilaga:

- Bilaga A – Ks § 155

I förslaget görs ingen ändring av syskonrabatten, vilket var förslaget i tidigare förslag. Det är också möjlighet att ha kvar förundervisningen på 4 h/dag, men skulle öka på behovet av administration.



Differensen i avgiftsintäkter är följande vad gäller förundervisningen:

60% vårdtid: -28,80

80% vårdtid: -26,60

100% vårdtid: -24,00

Utbildningschefen förordar

Kommunstyrelsen beslutar att barnomsorgsavgifterna och avgiftstillämpningen från och med 1.1.2025 för kommunens daghem fastställs enligt bilaga.

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att barnomsorgsavgifterna och avgiftstillämpningen från och med 1.1.2025 för kommunens daghem fastställs enligt Bilaga A – Ks § 155.



156 § Fritidshemstaxa (Dnr: 267/2024)

Ks § 156/6.11.2024

Ingen ändring föreslås i fritidshemstaxan inför nästa år. Förslag till taxa, enligt bilaga:

- Bilaga A – Ks § 156

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att fastställa fritidshemstaxan enligt Bilaga A – Ks § 156 att gälla från 1.1.2024



157 § Äldreomsorgsförvaltningens avgifter (Dnr: 268/2024)

Ks § 157/6.11.2024

Stödservicetaxan föreslås höjas med två procent. I övrigt föreslås inga ändringar. Förslag till avgifter, enligt bilaga:

- Bilaga A - Ks § 157

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna äldreomsorgsförvaltningens avgifter enligt Bilaga A - Ks § 157 att gälla från 1.1.2025.



158 § Skolans hyrestaxor (Dnr: 269/2024)

Ks § 158/6.11.2024

Utbildningschefens beredning

Hyrestaxorna i Lumparlands skola föreslås justeras med 2,0 % jämfört med 2024.

Förslag till hyrestaxor för Lumparlands skola fr.o.m. 1.1.2025, enligt bilaga:

- Bilaga A – Ks § 158

Utbildningschefen förordar

Kommunstyrelsen föreslår för kommunfullmäktige att bifogat förslag till hyrestaxor i Lumparlands skola godkänns.

Kommundirektörens förslag

Kommunstyrelsen beslutar att godkänna hyrestaxor i Lumparlands skola enligt Bilaga A – Ks § 158 att gälla från och med 1.1.2025.



159 § Snöplogningsavgift för privatkunder år 2025, Lumparland (Dnr: 270/2024)

Tn § 72/19.9.2024

Privatvägsplogningen har ca. 40 abonnenter och ska kostnadsfritt vara självbärande för kommunen. Ledamot Gun Nordqvist-Alm anmäler jäv och avlägsnar sig ifrån rummet.

Tekniska chefens förslag

Tekniska nämnden föreslår att man följer inflationen, och höjer privata snöplogningsavgiften i Lumparland med 3% (enligt bilaga).

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag. Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Bilagor

Snöplogningsavgift_2025_lu (4)

Ks § 159/6.11.2024

Förslag till snöplogningsavgift, enligt bilaga:

- Bilaga A – Ks § 159

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att godkänna snöplogningsavgiften enligt Bilaga A – Ks § 159 att gälla från och med 1.10.2025.



160 § Taxa bilplats med eluttag 2025, Lumparland (Dnr: 271/2024)

Tn § 69/19.9.2024

Kommunen har totalt 18 bilplatser som är utrustade med eluttag. Eluttagen är i huvudsak uthyrda till kommunens personal. För tillfället är ungefär hälften av platserna reserverade. Hyran har varit 29,08 €/år (exkl. moms), 36,06 €/år (inkl. 24% moms) för år 2024.

Tekniska chefens förslag

Tekniska nämnden föreslår för kommunstyrelsen att avgiften för bilplatser med eluttag höjs med cirka 2 % till 29,66 €/år (exkl. moms), 37,22 €/år (inkl. 25,5% moms) för år 2025. Höjningen motiveras med stigande konsumentprisindex.

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag.

Ks § 160/6.11.2024

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att avgiften för bilplatser med eluttag höjs med cirka 2 % till 29,66 €/år (exkl. moms), 37,22 €/år (inkl. 25,5% moms) från 1.1.2025. Höjningen motiveras med stigande konsumentprisindex.



161 § Vattenanslutningsavgift år 2025, Lumparland (Dnr: 272/2024)

Tn § 62/19.9.2024

Gällande vattenanslutningstaxa år 2024 är:

Grundavgift per fastighet, 2081€

Därtill per lokal, 520€

Tekniska chefens förslag

Tekniska nämnden beslutar att föreslå en höjning med 2% på vattenanslutningstaxan år 2025. Gällande taxa för år 2025

-Grundavgift per fastighet, 2123 €

-Därtill per lokal, 530 €.

Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag.

Ks § 161/6.11.2024

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige en höjning med 2% på vattenanslutningstaxan år 2025. Gällande taxa för år 2025:

-Grundavgift per fastighet, 2123 €

-Därtill per lokal, 530 €.



162 § Avloppsanslutningsavgift år 2025, Lumparland (Dnr: 273/2024)

Tn § 63/19.9.2024

Gällande taxa för år 2024-Grundavgift per fastighet, 2255 €-Därtill per lokal, 485 €.

Tekniska chefens förslag

Tekniska nämnden beslutar att föreslå en höjning med 2% på avloppsanslutningstaxan år 2025. Gällande taxa för år 2025-Grundavgift per fastighet, 2300 €-Därtill per lokal, 495 €. Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag.

Ks § 162/6.11.2024

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige en höjning med 2% på avloppsanslutningstaxan år 2025. Gällande taxa för år 2025:

-Grundavgift per fastighet, 2300 €

-Därtill per lokal, 495 €.



163 § Avloppsvattentaxa år 2025, Lumparland (Dnr: 274/2024)

Tn § 59/19.9.2024

Kommunen har ett allmänt avloppsvverk som emottar avloppsvatten för vidare transport från abonnenten till reningsverket i Långnäs. För att täcka kostnaderna uppbärs avgifter i form av anslutningsavgifter samt förbrukningstaxor för dessa tjänster.

Verksamheten regleras av LL om allmänna vatten- och avloppsnät samt LL om avloppsvattentaxa. Enligt LL om ändring av 5 § i lagen om avloppsvattenavgift (ÅFS 56/05) "skall bruksavgiften senast den 31.12.2010 på grund av den mängd vatten som används i fastigheten fastställas så att avgiften täcker kostnaderna för vattentjänsten". Lagen trädde i kraft den 1.1.2006. Sedan 2018 är avskrivningarna med i budgeten för att ge en korrekt bild av kostnaderna.

Till kommunens avloppsnät är i dagens läge 56 fastigheter anslutna. Antalet stiger kontinuerligt. Taxa innefattande detaljerade grunder för fastställande av avloppsvattenavgift godkänns av kommunens fullmäktige. Kommunen har de senaste åren inte uppnått kostnadstäckning för avloppsvattentjänsten.

Tekniska chefens förslag

Med hänsyn till den generella inflationen som råder beslutar nämnden föreslå för kommunstyrelsen en höjning av avloppsvattentaxan med 3%. Det innebär att den nya avloppsvattentaxan från och med 01.01.2025 är 5,38 €/m³ (exkl. moms), 6,59 €/m³ (inkl. moms 25,5%).

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag. Nämnden påvisar dock att full kostnadstäckning för avloppsvatten ej kommer att uppfyllas. Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Bilagor

uträkning_avloppsvattentaxa_lu_ar_2025 (2)

Ks § 163/6.11.2024

Uträkning av avloppsvattentaxan, enligt bilaga:

- Bilaga A – Ks § 163

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige en höjning av avloppsvattentaxan med 3%. Det innebär att den nya avloppsvattentaxan från och med 1.1.2025 är 5,38 €/m³ (exkl. moms), 6,59 €/m³ (inkl. moms 25,5%).



164 § Renvattentaxa år 2025, Lumparland (Dnr: 275/2024)

Tn § 57/19.9.2024

Renvattentaxa uppbärs för att täcka kommunens kostnader för inköp och distribution av renvatten i kommunen. Verksamheten är frivillig och momspliktig.

Vi har i dagens läge cirka 240 abonnenter. Totalt berörs ca 520 personer av vattendistribution (inklusive fritidshusen).

Enligt LL om ändring av 13 § i lagen om allmänna vatten- och avloppsverk (ÅFS 55/05)

"skall priset på hushållsvatten som distribueras från vattenverk senast den 31.12.2010

bestämmas så att intäkterna täcker kostnaderna för vattentjänsten".

Lagen trädde i kraft den 1.1.2006.

Sedan 2018 är avskrivningar med i budgeten för att ge en korrekt bild av kostnaderna.

Ålands vatten har aviserat en höjning av renvattenpriset om 5%. Enligt aviseringen skall förslaget till justerat pris behandlas i november. Beräkningen av kommunens renvattentaxa har beräknats utgående från en höjning om 5% på levererat renvatten från Ålands Vatten.

Då inte taxan för grundavgiften och hyran för vattenmätare höjts på flera år, finns det skäl att även höja med 2% även här. Det hjälper till för att uppnå kostnadstäckning. Då täcker de förväntade intäkterna de förväntade utgifterna. Det beräknade överskottet blir då 1353€.

Tekniska chefens förslag

Tekniska chefen föreslår för tekniska nämnden att renvattentaxan höjs med 5% till 1,81 €/m³ (exkl. moms, 2,27 €/m³ (inkl. 25,5% moms). Grundavgiften höjs med 2% till 85,39 €/år (exkl. moms), 107,17 €/år (inkl. 25,5% moms). Mätarhyror höjs med 2% enligt följande:

Q3=4, 6,30 €/år (exkl. moms), 7,90 €/år (inkl. 25,5% moms)

Q3=10, 12,40 €/år (exkl. moms), 15,57 €/år (inkl. 25,5% moms)

Q3=16, 24,81 €/år (exkl. moms), 31,13 €/år (inkl. 25,5% moms)



Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag. Ärendets behandling fortsätter i kommunstyrelsen i Lumparland.

Ks § 164/6.11.2024

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige att renvattentaxan höjs med 5% till 1,81 €/m³ (exkl. moms), 2,27 €/m³ (inkl. 25,5% moms). Grundavgiften höjs med 2% till 85,39 €/år (exkl. moms), 107,17 €/år (inkl. 25,5% moms). Mätarhyror höjs med 2% enligt följande:

Q3=4, 6,30 €/år (exkl. moms), 7,90 €/år (inkl. 25,5% moms)

Q3=10, 12,40 €/år (exkl. moms), 15,57 €/år (inkl. 25,5% moms)

Q3=16, 24,81 €/år (exkl. moms), 31,13 €/år (inkl. 25,5% moms)



165 § Lägenhetshyror år 2025, Lumparland (Dnr: 276/2024)

Tn § 71/19.9.2024

Lumparlands kommunen har totalt 18 bostadslägenheter. Lägenheterna är belägna i tre separata radhus på Kapellhagenområdet i Klemetsby samt nybyggda parhuslägenheter på Fjärilsgränd 2. Parhuslägenheterna är ännu inte uthyrda och kommer därför inte att omfattas i det här ärendet. Uthyrningssituationen är bra, samtliga lägenheter är uthyrda och lägenheter som blir uppsagda blir uthyrda snabbt igen. Tillsättandet av hyresgäster för bostadslägenheterna görs av kommunstyrelsen/kommundirektören i Lumparland. Hyrorna uppbärs av tekniska kansliet.

Tekniska nämndens roll i övrigt är att fungera som förvaltare/disponent för byggnaderna och gentemot hyresgästerna. Den löpande fastighetskötseln sköts av egen personal.

Hyran bestäms enligt vad som avtalats om inte något annat följer av denna eller annan lag... HL 11 § (ÅFS 19/99)

Hyresvärden i ett hyresförhållande som uppkommit innan denna lag trädde ikraft (1.7.1999) får årligen höja hyran med ett belopp som motsvarar förändringen i konsumentprisindex för Åland sedan denna lag trädde ikraft... HL 110 § (ÅFS 19/99).

Konsumentprisindex i juli 2024 var enligt statistikcentralen 3,0 %.

Tekniska chefens förslag

Med hänsyn till den generella inflationen som råder beslutar nämnden föreslå för kommunstyrelsen en höjning av hyrorna i radhusen vid Prästgårdsvägen 5 7 samt Kapellvägen 2 med 3%.

- Hyran för lägenheterna i Prästgårdsvägen 5-7 höjs från 6,78 €/m² till 6,98 €/m².

- Hyran för lägenheterna i Kapellvägen 2 höjs från 8,24 €/m² till 8,49 €/m².

Beslut

Tekniska nämnden beslöt enhälligt att omfatta tekniska chefens förslag.

Ks § 165/6.11.2024

Kommundirektörens förslag

Kommunstyrelsen beslutar föreslå fullmäktige en höjning av hyrorna i radhusen vid Prästgårdsvägen 5 7 samt Kapellvägen 2 med 3%. Detta med hänsyn till den generella inflationen.



-
- Hyran för lägenheterna i Prästgårdsvägen 5-7 höjs från 6,78 €/m² till 6,98 €/m².
 - Hyran för lägenheterna i Kapellvägen 2 höjs från 8,24 €/m² till 8,49 €/m².



**166 § Kapacitetsreservering Lotsbroverket, Lumparland (Dnr:
239/2024)**

Tn § 85/31.10.2024

Kompletteras efter tekniska nämndens behandling.



167 § Utlåtande VA-plan Åland 2025-2040 (Dnr: 251/2024)

Tn § 86/31.10.2024

Kompletteras efter tekniska nämndens behandling.



168 § Marknadsföring av kommunen (Dnr: 188/2023)

Ks § 117/20.9.2023

Det har under en tid diskuterats i kommunstyrelsen hur man skulle kunna gå tillväga för att marknadsföra kommunen på ett bättre sätt. Ärendet är speciellt aktuellt med tanke på byggnationen av nya lägenheter i kommunen.

I enlighet med dessa diskussioner har kommunstyrelsens ordförande, kommunfullmäktige I vice ordförande och kommundirektören varit i kontakt med produktionsbolag för att eventuellt skapa en marknadsförande film om Lumparlands kommun.

Uppskattningsvis kostar en produktion av en kortare film om Lumparland inte mer än 5 000 euro. För att få med så mycket som möjligt i filmen bör den produceras över ett år och skulle därför bli klar tidig höst 2024.

Kommundirektörens förslag

Kommunstyrelsen beslutar ta ställning till huruvida medel i budget 2024 ska tas upp för produktionen av en marknadsförande film om Lumparlands kommun.

Beslut

Kommunstyrelsen beslöt enhälligt att medel på 5 000 euro tas upp i budgetförslaget 2024 för produktion av en marknadsförande film om Lumparlands kommun.

Ks § 168/6.11.2024

En film har framtagits av From the Island och är klar att distribueras genom lämpliga kanaler. Filmen vissas vid sammanträdet.

Kommunstyrelsen har som ansvar för marknadsföring av kommunen och bör besluta om i vilka kanaler kommunen ska använda filmen.

Några olika alternativ skulle kunna vara följande:

- Publicera filmen på kommunens webbplats samt på sociala medier som Facebook.
- Samarbeta med Visit Åland eller Åland Living då de når en bredare publik med intresse för regionen.
- Be om hjälp från skolor, föreningar och andra organisationer att sprida filmen till sina medlemmar och nätverk.
- Visa filmen på skärmar i kommunens lokaler. Detta kräver dock fler skärmar.



-
- Inkludera länken till filmen i Infobladet.

Kommundirektörens förslag

Kommunstyrelsen beslutar om följande kanaler för spridning av filmen:

- Publicera filmen på en lämplig plats på kommunens webbplats samt på Facebook.
- Ta kontakt med Visit Åland eller Åland Living.
- Översänd filmen till lokala föreningar samt Långnäs hamn i syfte att filmen sprids i deras nätverk.



169 § Förfrågan om besvär över KEVA:s utjämningsavgifter (Dnr: 277/2024)

Ks § 169/6.11.2024

Mellan de åländska kommunernas förvaltningar har det diskuterats om möjligheten att gemensamt besvara sig mot KEVAs uträkning av utjämningsavgifterna. För Lumparlands kommuns del har denna avgift stigit med cirka 100 procent. Det huvudsakliga skälet för ett besvär är att KEVA felaktigt jämför landskapsandelar med statsandelar.

Sunds kommun har föreslagits att samordna ett besvär genom att anlita en jurist för ändamålet. För att med framgång driva ett besvär har diskuterats att anlita extern jurist för att formulera besvärsskriften till ett maximibelopp om 10 000 euro, där summan dock troligen skulle bli lägre än så. För Lumparlands kommuns del skulle det röra sig om cirka 100–150 euro om alla kommuner skulle vara med på besväret och kostnaden skulle fördelas enligt befolkningsmängd.

Frågan har diskuterats huruvida det ska göras som en gemensam talan eller där kommunerna endast finansierar Sunds kommuns besvär. Det bör vara bättre att vara med som besvärande så att eventuellt gynnande beslut direkt berör Lumparlands kommun. Enligt förvaltningsstadgan är det kommunstyrelsen som anför besvär.

Kommundirektörens förslag

Kommunstyrelsen beslutar att meddela Sunds kommun att Lumparlands kommun vill delta i en gemensam talan med Sunds kommun och eventuella övriga kommuner vad beträffar besvär över KEVAs utjämningsavgifter till ett maximibelopp om 150 euro för Lumparlands kommuns del. Kommundirektören befullmäktigas att vidta behövliga åtgärder för att delta i besväret.



170 § Lagförslag om landskapslag om cybersäkerhet och motståndskraft (Dnr: 256/2024)

Ks § 170/6.11.2024

Landskapsregeringen ger Lumparlands kommun möjlighet att lämna synpunkter på lagförslaget om landskapslag om cybersäkerhet och motståndskraft, senast 18.11.2024. Lagförslag, enligt bilaga:

- Bilaga A – Ks § 170

Syftet med lagförslaget är att inom landskapet genomföra Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) samt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG. Dessa direktiv syftar till att höja säkerhetsnivån för nätverks- och informationssystem samt att stärka motståndskraften i kritiska samhällsverksamheter.

Med anledning av detta behöver Lumparlands kommun ta ställning till hur lagförslaget kan påverka kommunens verksamheter, vilka konsekvenser och åtgärder det medför samt avge ett yttrande till Ålands landskapsregering.

Bakgrund till lagförslaget

Den snabba digitaliseringen av samhället har medfört nya utmaningar och risker för säkerheten i nätverks- och informationssystem, vilket gör att robusta säkerhetslösningar och förbättrade rutiner för riskhantering krävs för att skydda såväl verksamhetskritiska tjänster som samhällsstrukturen i stort. NIS 2-direktivet och CER-direktivet har antagits för att skapa en gemensam ram inom EU som stärker cybersäkerheten och motståndskraften mot störningar, inklusive både fysiska och digitala hot.

NIS 2-direktivet ersätter det tidigare NIS 1-direktivet och syftar till att höja den gemensamma säkerhetsnivån inom EU genom att ställa högre krav på säkerheten i nätverks- och informationssystem för samhällskritiska tjänster. Det utvidgar också direktivets tillämpningsområde till fler sektorer och skärper kraven för att hantera cyberhot.

CER-direktivet, som är nytt, kompletterar NIS 2-direktivet genom att säkerställa att kritiska verksamhetsutövare, både offentliga och privata, kan hantera såväl cyberattacker som fysiska störningar, exempelvis naturkatastrofer eller terrorattacker. Direktivet siktar på att öka motståndskraften hos viktiga samhällsverksamheter som levererar nödvändiga tjänster till samhället.



Sammanfattning av lagförslagets innehåll

Lagförslaget innebär att verksamheter inom flera samhällskritiska sektorer omfattas av krav på förbättrad cybersäkerhet och motståndskraft. De sektorer som berörs innefattar bland annat:

- Energi
- Transport
- Hälsa- och sjukvård
- Dricksvatten och avloppsvatten
- Digital infrastruktur
- Offentlig förvaltning

För att säkerställa dessa verksamheters funktioner införs krav på att alla berörda verksamhetsutövare implementerar robusta riskhanteringssystem. Det inkluderar:

1. **Riskbedömning:** Verksamheter måste genomföra en kontinuerlig bedömning av risker relaterade till deras nätverks- och informationssystem samt fysiska säkerhet.
2. **Incidentrapportering:** Alla incidenter som påverkar verksamheten eller nätverken ska rapporteras till en ansvarig myndighet inom en viss tidsram. Vid allvarliga incidenter krävs omedelbar rapportering.
3. **Åtgärdsplaner:** Verksamheter måste utveckla och genomföra åtgärdsplaner för att hantera risker och säkra driften vid störningar.
4. **Kontinuerlig utbildning:** Verksamhetsutövare ska tillhandahålla utbildning för sina anställda för att säkerställa att de har nödvändig kunskap om cybersäkerhet och riskhantering.
5. **Säkerhet i leveranskedjan:** Verksamhetsutövare ska säkerställa att deras leverantörer och underleverantörer följer samma höga krav på cybersäkerhet och motståndskraft.

Tillsynsmyndighet över att verksamheter uppfyller lagens krav är landskapsregeringen, vilket kan vara problematiskt eftersom de också är rådgivande myndighet.

Påverkan på Lumparlands kommun

För Lumparlands kommun, som är en liten kommun med cirka 30 anställda och ett antal samhällsviktiga verksamheter som grundskola, daghem, serviceboende för äldre, reningsverk samt vatten- och avloppsledningar, innebär lagförslaget ett flertal skyldigheter.



Cybersäkerhet

De verksamheter som bedrivs inom kommunen, såsom skolor och äldreboenden, måste uppfylla de nya kraven på cybersäkerhet. Det innebär att kommunen behöver utveckla en strategi för cybersäkerhet, genomföra riskbedömningar och säkerställa att rätt tekniska åtgärder finns på plats för att skydda de informationssystem som används i verksamheterna. Det gäller särskilt informationssystem som hanterar känsliga data om elever, personal och boende.

Kritisk infrastruktur

Även om Lumparlands kommun inte har ett eget vattenverk omfattas kommunen av reglerna för avloppsvatten och vatten- och avloppsledning. Dessa funktioner är avgörande för att säkerställa att samhällsservicen fungerar utan avbrott, och därför behöver kommunen vidta nödvändiga åtgärder för att hantera eventuella risker kopplade till denna infrastruktur. Det kan handla om att utveckla beredskapsplaner för hur kommunen ska agera vid större störningar eller säkerhetsincidenter som påverkar vatten- och avloppssystemet.

Rapporteringsskyldigheter

Lumparlands kommun kommer att bli skyldig att rapportera allvarliga incidenter som påverkar kommunens verksamheter eller infrastruktur. Detta innefattar såväl cybersäkerhetsincidenter som fysiska störningar. Kommunen behöver därför säkerställa att det finns tydliga rutiner för hur incidenter ska identifieras, rapporteras och hanteras, samt vilken myndighet som ansvarar för tillsyn och samordning.

Ekonomiska konsekvenser

Införandet av den nya lagen kommer sannolikt att innebära ökade kostnader för Lumparlands kommun. Investeringar i både teknik och personal kommer att vara nödvändiga för att säkerställa att kommunen kan möta de nya kraven. Det kan handla om att uppgradera befintliga system för att förbättra cybersäkerheten, att införa nya rutiner för riskhantering samt att utbilda personal inom alla verksamheter som berörs.

Samverkan och stöd

För att implementera lagförslaget kan det vara nödvändigt för kommunen att söka samverkan med andra kommuner eller med myndigheter som har specialkompetens inom cybersäkerhet och beredskap för kritisk infrastruktur. Detta kan underlätta för mindre kommuner som Lumparland att uppfylla de nya kraven utan att själva behöva utveckla all kompetens internt.

Kommundirektörens förslag

Kommunstyrelsen beslutar konstatera att lagförslaget bygger på EU-direktiv och således är nödvändigt att införa och har således inte några direkta synpunkter på lagförslaget. Det är dock väsentligt att landskapsregeringen



erbjuder utbildnings- och diskussionstillfällen kring vad lagarna innebär i praktiken.

Kommunstyrelsen beslutar vidare att Lumparlands kommun ställer sig bakom alla former av samarbeten för att uppfylla lagförslagets krav och att lagförslaget oundvikligen kommer medföra ökade kostnader och administration för kommunen.



171 § Sammanträdet avslutande

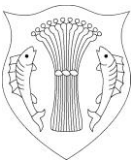
Sammanträdet avslutades kl. XX.XX.

Intagningsprinciper för Kapellhagen

-Ett serviceboende med heldygnsomsorg

Lumparlands kommun





INNEHÅLLSFÖRTECKNING

1. Personer som fyllt 65 år.....	2
2. Definition av vård-och omsorgsbehov	2
3. Vård- och omsorgsbehov nattetid.....	2
4. Vård-och omsorgsbesök som överstiger 38 timmar per månad.....	2
5. Äldre med minnesproblematik	2
6. Service i hemmet.....	2
7. Hembesök.....	3
8. Period- och avlastningsplats	3
9. Kartläggning av vård-och omsorgsbehovet	3
10. Väntelista.....	3
11. Ansvarsperson för uthyrning.....	3



Antagna av kommunstyrelsen genom § 22/31.1.2024.

1. PERSONER SOM FYLLT 65 ÅR

Lägenheter på serviceboendet med heldygnsomsorg Kapellhagen hyrs ut till personer som fyllt 65 år, här nedan kallat den äldre.

2. DEFINITION AV VÅRD- OCH OMSORGSBEHOV

Med vård- och omsorgsbehov menas regelbunden hjälp med de dagliga rutinerna såsom hjälp med den personliga hygien, toalettbesök, av- och påklädning, hjälp vid måltider, hjälp/stöd att förflytta sig inomhus och utomhus samt tillsynsbesök.

3. VÅRD- OCH OMSORGSBEHOV NATTETID

En förutsättning för att en äldre ska kunna hyra en lägenhet på Kapellhagen är att den äldre har ett sådant vård- och omsorgsbehov att denne kan vårdas i ett olåst boende nattetid.

4. VÅRD- OCH OMSORGSBESÖK SOM ÖVERSTIGER 38 TIMMAR PER MÅNAD

Den äldres vård- och omsorgsbehov är sådant att denne har behov av hemservicebesök som överstiger 38 timmar per månad och som inkluderar besök nattetid. Akut sjukdom/vårdbehov kan också ligga till grund för intagning till Kapellhagen.

Vård- och omsorgsbehovet därmed att den äldre har behov av hemservice 38 timmar per månad eller fler. De boende på Kapellhagen debiteras således den högsta hemserviceavgiften i enlighet med gällande boendeservicetaxa.

5. ÄLDRE MED MINNESPROBLEMATIK

Lägenheter hyrs ut till äldre med minnesproblematik men för äldre som är rymnings- och utåtagerande erbjuds andra vårdalternativ.

6. SERVICE I HEMMET

För de äldre som har ett vård- och omsorgsbehov understigande 38 timmar per månad dagtid och inget behov av besök nattetid och för de äldre som i huvudsak har behov av hjälp i hushållet och stödservicetjänster såsom måltids- och klädvårdservice erbjuds hemservice i hemmet alternativt kombinerat med momsfri socialservice.



7. HEMBESÖK

Ledande personal inom äldreomsorgen gör hembesök till den äldre för att tillsammans med pensionären och eventuella anhöriga/närstående utreda huruvida vård- och omsorgsbehovet är i enlighet med gällande principer för uthyrning av lägenheter på **ESB** Kapellhagen.

8. PERIOD- OCH AVLASTNINGSPLATS

För periodplats finns en lägenhet som kan användas i enlighet med gällande boendeservicetaxa. Periodplats debiteras enligt taxa för "stödservice och fasta avgifter" alternativt "enligt taxa för kortvarig vård".

Periodplatsen hyrs i första hand till äldre som blivit utskrivna från sjukhus och som behöver en viss tids rehabilitering samt till vårdtagare som vårdas av närståendevårdare i form av lagstadgad avlastning för närståendevårdaren.

9. KARTLÄGGNING AV VÅRD-OCH OMSORGSBEHOVET

För att kartlägga omfattningen och frekvensen av vård- och omsorgsbehovet eller huruvida pensionärens behov av vård- och omsorg kan ombesörjas på Kapellhagen, hyr den äldre den tilltänkta lägenheten eller periodplatslägenheten som en periodplats under högst två månaders tid i enlighet med gällande boendeservicetaxa. Lägenhet hyrs ut varaktigt efter en periodplatsperiod om minst två veckor.

10. VÄNTELISTA

Då samtliga lägenheter är uthyrda på Kapellhagen uppgörs en väntelista. När en lägenhet blir ledig och ska fördelas prioriteras alltid vård- och omsorgsbehovet framom inskrivning på väntelista eller antecknad väntetid. De äldre som har behov av hemservicebesök som överstiger 38 timmar per månad och som inkluderar besök nattetid samt de som vårdas via närståendevård prioriteras.

11. ANSVARSPERSON FÖR UTHYRNING

Valet av hyresgäst avgörs av äldreomsorgschefen i enlighet med kommunstyrelsens delegeringsordning. Äldreomsorgschefen är även ansvarsperson för uppgörande av hyresavtal samt väntelista.

AVTAL OM FÖRSÄLJNING AV TJÄNSTER INOM KOMMUNAL INFRASTRUKTUR, BYGGNADSTILLSYN, BEFOLKNINGSSKYDD SAMT SKÖTSEL AV ANLÄGGNINGAR OCH FASTIGHETER

1. Parter

Lemlands kommun (FO-nummer: 0205034-3)
Kommunrundan 7, AX-22 610 Lemland
(nedan "säljaren"); och

Lumparlands kommun (FO-nummer: 0205038-6)
Kyrkvägen 26, AX-22 630 Lumparland
(nedan "köparen")

2. Föremål för avtalet

Parterna avtalar härmed om köp och försäljning av berednings-, besluts- och verkställighetstjänster inom kommunal infrastruktur, byggnadstillsyn, befolkningskydd samt skötsel av anläggningar och fastigheter för sedvanlig driftverksamhet. Avtalet omfattar inte köp och försäljning av tjänster för investeringsprojekt.

Detta avtal är upprättat med stöd av 78 § kommunallagen (ÅFS 1997:73) för landskapet Åland eller motsvarande senare lagstiftning.

Till den del avtalet omfattar byggnadstillsyn är avtalet upprättat i enlighet med 14 § 3 mom. plan- och bygglag (ÅFS 2008:102) för landskapet Åland eller motsvarande senare lagstiftning.

Lemlands och Lumparlands kommuner har med detta avtal kommit överens om att Lumparlands kommun anförtror Lemlands kommun att sköta vissa fördefinierade uppgifter för Lumparlands kommuns räkning.

Lemlands och Lumparlands kommuner har med detta avtal kommit överens om att sådana uppgifter inom kommunal infrastruktur och byggnadstillsyn som enligt lag ska skötas av kommunen och som kan delegeras till en tjänsteman anförtros från Lumparlands kommun till vissa fördefinierade anställda som står i tjänsteförhållande hos Lemlands kommun, vilka sköter uppgiften under tjänstemannaansvar.

Avtalet reglerar försäljning av berednings-, besluts- och verkställighetstjänster inom kommunal infrastruktur, byggnadstillsyn och befolkningskydd från Lemlands kommun och fastställer rättigheter, skyldigheter samt leverans- och betalningsvillkor för båda parterna.

3. Bakgrund

Lemlands och Lumparlands kommuner har haft ett omfattande samarbete avseende nämnder och övrig myndighetsutövning inom kommunal infrastruktur, byggnadstillsyn och befolkningskydd samt skötsel av anläggningar och fastigheter under perioden 2012–2024.

I samband med att det tidigare samarbetsavtalet har sagts upp har kommunerna gemensamt undersökt om det finns synergieffekter och förutsättningar för Lemlands kommun att sälja tjänster inom kommunal infrastruktur, byggnadstillsyn, befolkningskydd samt skötsel av anläggningar och fastigheter.

Beredning som har lett fram till detta avtal har skett i dels samarbetskommittén mellan Lemlands och Lumparlands kommuner under första halvan av år 2024, dels internt inom Lemlands kommun.

4. Försäljningens omfattning

Tjänsten omfattar alla faser av beredning, föredragning, beslut och verkställighet exklusive fakturering inom sedvanlig driftverksamhet för kommunal infrastruktur, byggnadstillsyn, befolkningskydd samt skötsel av anläggningar och fastigheter. Säljaren producerar tjänsterna till köparen integrerat och likvärdigt med motsvarande uppgifter som säljaren utför för driften inom den egna kommunen.

Säljaren förbinder sig att leverera tjänster enligt följande:

- a. Kommunal infrastruktur uppgående till högst 21,45 h/vecka i medeltal under ett kalenderår (*teknisk chef, kommuntekniker och administratör eller motsvarande senare roller*). I detta ingår möjlighet att tekniska chefen är föredragande i en teknisk nämnd eller motsvarande organ hos köparen.
- b. Byggnadstillsyn och befolkningskydd uppgående till högst 11,00 h/vecka i medeltal under ett kalenderår (*byggnads- och miljöinspektör och administratör eller motsvarande senare roller*). I detta ingår möjlighet att byggnads- och miljöinspektören är föredragande i en byggnadsnämnd eller motsvarande organ hos köparen.
- c. Skötsel av anläggningar och fastigheter uppgående till högst 40,50 h/vecka i medeltal under ett kalenderår (*fastighetsskötare och serviceskötare eller motsvarande senare roller*).

Köparen förbinder sig att köpa tjänster enligt följande:

- d. Kommunal infrastruktur uppgående till minst 11,00 h/vecka i medeltal under ett kalenderår (*teknisk chef, kommuntekniker och administratör eller motsvarande senare roller*).
- e. Byggnadstillsyn och befolkningskydd uppgående till minst 7,50 h/vecka i medeltal under ett kalenderår (*byggnads- och miljöinspektör och administratör eller motsvarande senare roller*).
- f. Skötsel av anläggningar och fastigheter uppgående till minst 38,25 h/vecka i medeltal under ett kalenderår (*fastighetsskötare och serviceskötare eller motsvarande senare roller*).

Om säljarens kapacitet tillfälligt underskrider uppskattningen av tjänsternas omfattning enligt detta avtal kan köparen och säljaren komma överens om en tidsbunden minskning av resurserna enligt villkoren i detta avtal.

Om köparens behov av tjänster tillfälligt överstiger uppskattningen av tjänsternas omfattning enligt detta avtal kan köparen och säljaren komma överens om en tidsbunden utökning av resurserna enligt villkoren i detta avtal.

Säljaren förbehåller sig rätten att avsäga sig uppdrag som till arbetsmängden enligt säljarens bedömning väsentligen överskrider omfattningen av tjänster enligt villkoren i detta avtal.

Parterna ska årligen, senast under september månad, föra en dialog om antalet timmar som avtalet omfattar inför kommande verksamhetsår. Vid dialogen kan parterna komma överens om att försäljningens omfattning antingen ska bibehållas, ökas eller minskas.

Köparen ansvarar för initiativ och beställning av tjänster från externa parter enligt köparens bedömning av kompetensbehov och resurs samt eventuella krav som ställs på köparen som myndighet i den lagstiftning som ska tillämpas.

Köparen ansvarar för att sådana beslut som inte har delegerats till en anställd tjänsteman hos säljaren kan fattas i behörigt organ i kommunen.

Säljaren ansvarar för att avdela resurser som i huvudsak utgörs av säljaren anställd teknisk chef i tjänsteförhållande, kommuntekniker i tjänsteförhållande, byggnads- och miljöinspektör i tjänsteförhållande, administratör i arbetsavtalsförhållande, fastighetsskötare i arbetsavtalsförhållande samt serviceskötare i arbetsavtalsförhållande eller motsvarande senare roller, alternativt någon kombination av dessa funktioner och kompetenser.

Säljaren förbehåller sig rätten att, utgående från uppdragets art och säljarens bedömning av kompetensbehovet, avdela en lämplig resurs för respektive uppgift.

Användningen av lagerhållet material, verktyg och arbetsmaskiner i anslutning till utförandet av tjänsterna inom skötsel av anläggningar och fastigheter ska som utgångspunkt ersättas av köparen enligt säljarens självkostnadspris eller enligt separat överenskommelse.

5. Pris och betalningsvillkor

För upprätthållande av tjänsterna i detta avtal äger säljaren rätt att uppbära en grundavgift. Syftet med grundavgiften är att täcka den risk och det ansvar som säljaren bär samt en andel av de fasta avgifterna som säljaren oundvikligen har.

Tjänster faktureras per påbörjad timme enligt faktisk arbetsåtgång enligt säljarens redovisning.

Grundavgiften och timavgiften specificeras i den prislista som finns som bilaga till detta avtal.

Prissättningen revideras årligen så att säljaren senast 15 november året innan meddelar priserna för följande kalenderår. Vid väsentliga ändringar i grunderna för prissättningen kan priset revideras under pågående år enligt separat överenskommelse.

Priserna baserar sig på säljarens personalkostnader samt därtill hörande kostnader för utförande av tjänsterna, så som exempelvis nödvändig utrustning och IT-lösningar, och anges exklusive moms.

Säljaren fakturerar köparen kvartalsvis i förskott för grundavgiften samt för det minsta antalet timmar som köparen ska betala enligt punkterna 4d, 4e och 4f i detta avtal. Säljaren fakturerar därefter köparen kvartalsvis i efterskott utgående från förverkligat antal timmar.

Eventuella resekostnader tillkommer enligt Skattestyrelsens beslut om högsta skattefria reseersättningar.

6. Avtalsperiod och uppsägning

Detta avtal träder i kraft när de respektive parternas beslut om att godkänna avtalet har vunnit laga kraft och när det vederbörligen har undertecknats av parterna, dock så att avtalet tidigast träder i kraft från och med 1.1.2025.

Avtalet kan sägas upp av endera parten. Uppsägningstiden är 6 månader. Uppsägning av avtalet ska meddelas skriftligen. Parterna kan ömsesidigt komma överens om en kortare uppsägningstid.

7. Tystnadsplikt och sekretess

Parterna konstaterar att tystnadsplikt och sekretess ska beaktas i enlighet med gällande lagstiftning. Därtill ska säljaren följa sekretess- och tystnadsplikten för att skydda köparens affärshemligheter. Utan hinder för tystnadsplikt och sekretess äger parterna rätt att ta del av information som är nödvändig för utförandet av arbetet samt beslutsfattandet.

8. Arkivansvar

Köparen upprätthåller arkiv för de tjänster som ingår i detta avtal. Köparens arkiv ska vara tillgängligt för säljarens tjänstemän för sådana uppgifter som är nödvändiga för utförandet av arbetet samt beslutsfattandet.

9. Ändring och överlåtelse av avtal

Detta avtal kan inte överlåtas till tredje part utan parternas skriftliga godkännande. Ändring eller tillägg till detta avtal ska för att vara bindande göras skriftligen och undertecknas av samtliga parter.

10. Fel, sänkning av kostnader och förtida uppsägning

Köparen ska anmäla fel inom rimlig tid från det att felet uppdagades.

Säljaren ska därefter meddela åtgärder inom 14 dagar.

Båda parter har rätt att häva avtalet vid väsentligt avtalsbrott.

11. Force majeure

Parterna ska vara befriade från skyldigheter som följer av avtalet i det fall omständigheter inträder som ligger utanför parternas kontroll. Den part som vill påkalla force majeure ska meddela den andra parten om hindret och dess påverkan på fullföljandet av detta avtal.

12. Meningskiljaktigheter

Meningskiljaktigheter föranledda av detta avtal ska i första hand lösas genom förhandlingar mellan parterna.

Om parterna inte når samförstånd ska ärendet avgöras som ett tvistemål vid Ålands tingsrätt.

13. Datum och underskrift

Detta avtal är upprättat i två (2) likalydande exemplar, ett (1) vardera för parterna.

Lumparland den

Pia Eriksson
Kommunstyrelsens ordförande
Lumparlands kommun

Mattias Jansryd
Kommundirektör
Lumparlands kommun

Lemland den

Tony Asumaa
Kommunstyrelsens ordförande
Lemlands kommun

Julia Lindfors
Kommundirektör
Lemlands kommun

14. Bilagor

Till detta avtal fogas den prislista som Lemlands kommun har upprättat för försäljning av tjänsterna.

- a) Prislista för försäljning av tjänster inom kommunal infrastruktur, byggnadstillsyn samt skötsel av anläggningar och fastigheter för år 2025

**Prisbilaga till avtal om försäljning av tjänster inom kommunal infrastruktur,
byggnadstillsyn samt skötsel av anläggningar och fastigheter**

År 2025

<u>Grundavgift per månad</u>	<u>Pris exkl. moms</u>
Kommunal infrastruktur	1 600,00 €
Byggnadstillsyn	600,00 €
Skötsel av anläggningar och fastigheter	1 700,00 €

<u>Löpande kostnad per timme</u>	<u>Pris exkl. moms</u>
Ledande tjänster & myndighetsutövning	38,00 €
Administrativa tjänster	27,00 €
Fastighetskötsel	27,00 €

Resekostnader

Enligt Skattestyrelsens beslut

Budget 2025

Ekonomiplan 2026–27



Lumparlands kommun

Innehållsförteckning

1.	KOMMUNDIREKTÖRENS ÖVERSIKT	1
2.	ALLMÄNNA UPPGIFTER OM LUMPARLANDS KOMMUN	2
	2.1. Kommunens förvaltning.....	2
3.	INNEHÅLLET I OCH SAMMANDRAG AV BUDGETEN	3
	3.1. Budgetdirektiven	3
	3.2. Bindande nivåer	3
	3.3. Sammandrag av budget 2025	4
	3.4. Personal.....	5
	3.5. Investeringar	6
4.	FINANSIERINGSDELEN	7
	4.1. Resultaträkning	7
	4.2. Resultaträkning.....	9
	4.3. Finansieringsanalys	10
	4.4. Skatte kalkyl.....	11
	4.5. Landskapsandelar.....	11
5.	KOMMUNFULLMÄKTIGES VISION OCH MÅLSÄTTNINGAR.....	12
	5.1. Vision	12
	5.2. Verksamhetsmål 2025	12
	5.3. Verksamhetsmål 2026–2027	12
	5.4. Åtgärder för att uppnå de uppställda målen	12
6.	BUDGETFÖRUTSÄTTNINGAR	13
	6.1. Befolkningsuppgifter	13
	6.2. Skattesatser.....	14
	6.3. Landskapsandelar.....	14
	6.4. Kommunens skuldsättning	15
	6.5. Miljönyckeltal	15
	6.6. Personal.....	16
7.	DRIFTSEKONOMIN I DETALJ.....	19
	7.1. Centralförvaltningen.....	19
	7.2. Lantbruksnämnden.....	21
	7.3. Samordnad socialtjänst (Kommunernas socialtjänst k.f.)	22
	7.4. Äldreomsorgsförvaltningen.....	23
	7.5. Bildningsförvaltningen	25

7.6. Kultur- och fritidsförvaltningen.....	30
7.7. Byggnads- och miljönämnden.....	32
7.8. Tekniska nämnden	34
7.9. Brand- och räddningsväsendet (Ålands räddningsmyndighet)	40
8. INVESTERINGARNA.....	41



1. KOMMUNDIREKTÖRENS ÖVERSIKT

Av resultaträkningen för 2025 framgår att Lumparlands kommun förväntas uppvisa ett underskott på 596 861,80 euro med ett negativt årsbidrag på 432 043,80 euro. Det budgeterade underskottet och bristen på likvida medel fordrar att kommunen söker likviditetsstöd för att säkra likviditeten och samt upptar lån för alla investeringar.

Under 2025 förväntas kommunen att ta del av 779 497 euro i landskapsandelar inklusive kompensationer från landskapet. Det är i lägre än 2024, vilket är åt helt fel håll. Det behövs nämligen en väsentlig ökning av landskapsandelarna för Lumparlands kommuns del. Det är otvivelaktigt fortsättningsvis för lite finansiering från landskapet för kommunens lagstadgade service.

Skatteinkomsterna har senaste åren varit bättre än budgeterat men på grund av välfärdsområdesreformen i riket har skatteinkomsterna för 2023 och 2024 korrigerats under slutet av år 2024, vilket kraftigt bidragit till kommunens brist på likvida medel. Kommunen budgeterar 1 592 000 euro i totala skatteinkomster för 2025, vilket är mindre än budget 2024.

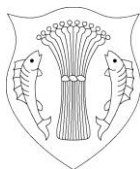
Investeringarna hålls på en relativt låg nivå, där planerade investeringar uppgår till 105 000 euro under 2025.

I budget 2025 ser vi främst kostnadsökningar inom äldreomsorgen, vilket har att göra med ett ökat tryck på serviceboende med heldygnsomsorg samt att kommunen inte längre hyr ut en plats till någon annan kommun, vilket kan vara ett sätt att få in inkomster om kommunen inte själv har behov av platsen.

Det är inte enbart Lumparlands kommun som just nu har en ekonomiskt svår situation, utan det är flertal kommuner som kommer söka likviditetsstöd och än fler som årligen visar stora underskott.

Budgeten för 2025 är inriktad på att bemöta ekonomiska utmaningar genom att prioritera kärnverksamheter och använda resurser effektivt. Lumparland ämnar fortsätta sin strävan att vara en självständig och attraktiv kommun för nuvarande och framtida invånare, men det är dock inte längre upp till kommunen själv, om landskapet antar en så kallad kriskommunlag och samtidigt fortsättningsvis ger för låga landskapsandelar till perifera kommuner.

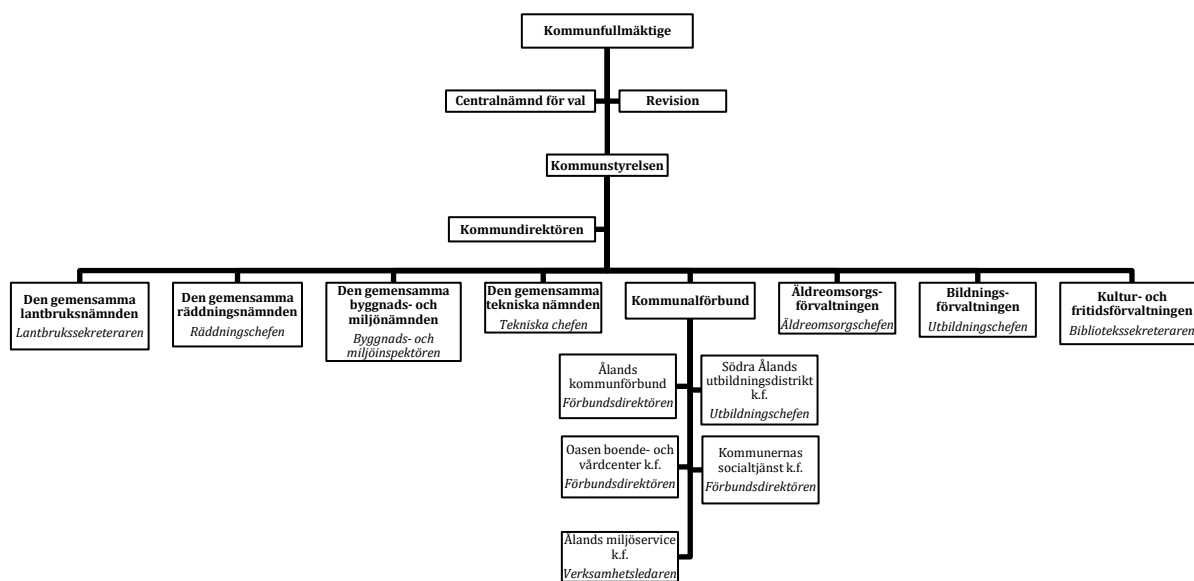
Mattias Jansryd



2. ALLMÄNNA UPPGIFTER OM LUMPARLANDS KOMMUN

Statistik	Bokslut 2023	Budget 2024	Budget 2025
Befolkning 31.12 enl. ÅSUB	366	366	367
Skattesats	19,50 %	19,50 %	19,50 %
Verksamhetens utgifter (1 000 euro)	2 990	-3 028	-3 233
Verksamhetens intäkter (1 000 euro)	427	331	555
Skatteinkomster (1 000 euro)	1 684	1 601	1 592
Skatteinkomster, euro/inv.	4602	4 374	4 338
Landskapsandel (1 000 euro)	820	826	779
Årsbidrag (1 000 euro)	-117	-385	-432
Avskrivningar (1 000 euro)	-167	-182	-165
Lån 31.12 (1 000 euro)	1968	2 817	2 795
Lån, euro/inv.	5377	7 697	7 614

2.1. Kommunens förvaltning



Kommunfullmäktige består av nio ledamöter för mandatperioden 2024–2027. Kommunstyrelsen består i sin tur av sex ledamöter med personliga ersättare. Därtill består kommunförvaltningen av nämnder och under kommunstyrelsen lydande förvaltningar samt nämnder som är gemensamma med andra kommuner. Kommunstyrelsen utses för två år i sänder. Nämnderna tillsätts för fullmäktiges mandatperiod.



3. INNEHÅLLET I OCH SAMMANDRAG AV BUDGETEN

3.1. Budgetdirektiven

Budgetdirektiven, godkända av kommunstyrelsen genom § 102/19.6.2024, utgår från budget 2024 med beaktande av den ekonomiska utvecklingen.

3.2. Bindande nivåer

3.2.1. Driftsekonomidelen

Budgetens nettobelopp för varje förvaltningsorgan är bindande gentemot kommunstyrelsen och budgetens totala nettobelopp är bindande gentemot kommunfullmäktige. Med beaktande av de målsättningar, eventuella begränsningar samt öronmärkta belopp som kommunfullmäktige fastställt i samband med att anslaget godkänts, får varje förvaltningsorgan göra omDispositioneringar mellan resultatenheterna. Kommunstyrelsen får i sin tur göra omDispositioneringar mellan förvaltningsorganen, även det med beaktande av de målsättningar, eventuella begränsningar samt öronmärkta belopp som kommunfullmäktige fastställt. Personalkostnader kan inte omDispositioneras för andra ändamål utan kommunfullmäktiges godkännande. Fullmäktige inrättar nya ordinarie tjänster och beslutar om utökning av ordinarie arbetstagare.

3.2.2. Investeringsdelen

Investeringsdelens anslag står till respektive förvaltningsorgans disposition för det projekt eller ändamål med de eventuella begränsningar som kommunfullmäktige fastställt i samband med att anslaget godkänts. Nettobeloppet är bindande gentemot kommunfullmäktige.

3.2.3. Resultaträkningsdelen

Kommunfullmäktige fastslår vilka anslag som följer efter verksamhetsbidraget som är bindande gentemot kommunfullmäktige. Planenliga avskrivningar som beräknats enligt avskrivningsplanen är inte bindande gentemot kommunfullmäktige.

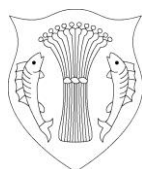
3.2.4. Finansieringsdelen

Poster som ska täcka ett finansieringsbehov eller utgöra överföring av finansieringsöverskott är bindande för kommunstyrelsen gentemot kommunfullmäktige.



3.3. Sammandrag av budget 2025

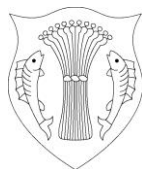
Sammandrag av förvaltningarna exkl. avskrivningar	Bokslut 2023	Budget 2024	Budget 2025	Förändring i %		Andel av skattesats
				mot 2024	Rel. andel i % 2024	
C100 Centralförvaltningen	-259 658,11	-275 619,90	-263 239,28	-4,49 %	9,83 %	1,92
C101 Lantbruk	-7 271,00	-10 821,00	-7 000,00	-35,31 %	0,26 %	0,05
C200 Samordnad socialtjänst	-337 853,86	-332 965,95	-372 000,00	11,72 %	13,89 %	2,71
C230 Äldreomsorgsförvaltningen	-702 481,74	-827 031,78	-943 080,78	14,03 %	35,21 %	6,87
C300 Bildningsförvaltningen	-907 632,76	-911 363,52	-890 993,72	-2,24 %	33,27 %	6,49
C400 Kultur- och fritidsförvaltningen	-48 748,06	-58 552,72	-56 905,10	-2,81 %	2,12 %	0,41
C500 Byggnads- och miljönämnden	-24 237,09	-25 659,00	-25 039,00	-2,42 %	0,93 %	0,18
C501 Tekniska nämnden	-235 286,79	-212 603,00	-87 128,00	-59,02 %	3,25 %	0,63
C600 Brand- och räddningsväsendet	-40 106,11	-42 909,00	-33 065,00	-22,94 %	1,23 %	0,24
C10 Driftshushållning Summa	-2 563 275,52	-2 697 525,87	-2 678 450,88	-0,71 %	100 %	19,50



3.4. Personal

	Budget 2024	Budget 2025
Centralförvaltningen	2,60	2,60
Kommundirektör	1,00	1,00
Ekonomichef	0,80	0,80
Byråsekreterare	0,80	0,80
Äldreomsorgsförvaltningen	12,73	12,15
Äldreomsorgschef*	0,30	0,30
Administratör*	0,30	0,30
Ledande närvårdare	1,00	1,00
Ställföreträdande ledande närvårdare	1,00	1,00
Närvårdare	6,87	6,35
"Pool"-resurs	0,50	0,50
Kock	0,80	0,80
Vikarier	1,96	1,90
Bildningsförvaltningen	10,45	11,53
<u>Barnomsorg</u>	<u>4,73</u>	<u>5,35</u>
Barnomsorgsledare*	0,13	0,13
Administratör*	0,13	0,13
Daghemsföreståndare	1,00	1,00
Lärare inom barnomsorg	1,00	1,00
Barnskötare	1,20	1,98
Lokalvårdare/köksbiträde	0,80	0,80
Vikarier	0,47	0,31
<u>Grundskola</u>	<u>5,72</u>	<u>6,18</u>
Skolföreståndare	1,00	1,00
Klasslärare i huvudsyssla	0,93	1,00
Timlärare i huvudsyssla	0,95	1,28
FBU-lärare	0,11	0,00
Assistent	0,54	0,77
Kock	1,00	1,00
Lokalvårdare/köksbiträde	1,00	1,00
Vikarier	0,19	0,13
Kultur-och fritidsförvaltningen	0,79	0,76
Bibliotek	0,50	0,50
Biblioteksvikarier	0,17	0,10
Ungdomsarbete	0,12	0,16
Byggnads- och miljönämnden*	0,35	0,20
Tekniska nämnden*	1,57	1,30
Brand- och räddningsväsendet*	0,05	0,02
Totalt	28,54	28,56

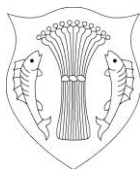
*Lumparlands del av den totala personalen



3.5. Investeringar

Investering	Budget 2025
8301 Hyresbostäder	
⊕ A4210 Inköp under räkenskapsperioden	-15 000,00
8304 Parhuslägenheter	
⊕ A4210 Inköp under räkenskapsperioden	-40 000,00
☐ C840 Övriga byggnader	
8302 Serviceboende Kapellhagen	
⊕ A4210 Inköp under räkenskapsperioden	-20 000,00
☐ C855 Maskiner och inventarier	
8558 Inventarier FBK	
⊕ A4210 Inköp under räkenskapsperioden	-10 000,00
☐ C880 Affärsverk	
8801 Vattendistributionsledningar	
⊕ A4210 Inköp under räkenskapsperioden	-10 000,00
8805 Avloppsledningar	
⊕ A4210 Inköp under räkenskapsperioden	-10 000,00
Totalsumma	-105 000,00

Investering	Plan 2026	Plan 2027
Inventarier FBK	- 15 000,00	
ESB Kapellhagen	- 20 000,00	- 20 000,00
Vattenledningar	- 10 000,00	- 10 000,00
Ospecificerade avloppsledningar	- 10 000,00	- 10 000,00
Hyresbostäder	- 15 000,00	
Båtbyte FBK	- 35 000,00	
Totalt	- 105 000,00	- 40 000,00



4. FINANSIERINGSDELEN

Kommunens finansieringsdel presenteras i form av en resultaträkning och en finansieringsanalys. Finansieringsanalysen utvisar finansieringsförändringarna och det beräknade penningflödet under budgetåret och hur finansieringen ordnas utgående från det förväntade resultatet i resultaträkningen. Resultaträkningen och finansieringsanalysen bildar således en ekonomisk helhetsbild av den ekonomiska situationen för kommunen.

Resultaträkningen bildas av poster från budgetens driftsdel och finansieringsdel.

4.1. Resultaträkning

Resultaträkningen innehåller nedan uppräknade poster.

4.1.1. Verksamhetens intäkter och kostnader

Verksamhetens intäkter och kostnader omfattar intäkter och kostnader från den löpande driftverksamheten, såsom försäljningsinkomster, avgifter, löner, kundtjänster etc.

4.1.2. Verksamhetsbidraget

Verksamhetsbidraget är alltid negativt och visar skillnaden mellan verksamhetsintäkter och verksamhetskostnader. Bidraget anger hur mycket den kommunala driftverksamheten kostar netto och vad som således ska finansieras med skatteinkomster, landskapsandelar och övriga finansiella inkomster.

4.1.3. Skatteinkomster

Visar det förväntade inflödet av skatter under året. Skatteinkomsterna utgörs av flera olika skatter.

4.1.3.1. Förvärvsinkomstskatt

Finlands kommunförbund gör i samarbete med Finansministeriet och Skatteförvaltningen en landsomfattande prognos för kommunernas skatteintäkter. Förvärvsinkomstskatten utgår från denna prognos med skattesatsen 19,5 %.

4.1.3.2. Fastighetsskatt

Fastighetsskatten utgår från Finlands kommunförbunds prognosverktyg. Skatten består av följande delar:

- Allmän för byggnader
- Allmän för markområden
- Stadigvarande boende
- Allmännyttiga samfund
- Obebyggd byggplats
- Kraftverk



4.1.3.3. Samfundsskatt

Samfundsskatten är svår att prognosticera då det är svårt att förutspå hur företagen kommer att agera. Viss återhållsamhet i prognoserna behövs då samfundsskatterna tidigare år har varit lägre än vad Finlands kommunförbund prognosticerat. Prognoserna baserar sig på skatteförvaltningens skattestatistik och de periodiska skatteredovisningarna.

4.1.3.4. Övriga skatteinkomster

Beloppet består av kommunens andel av på Åland influten källskatt.

4.1.4. Landskapsandelar

Landskapet deltar i finansieringen av kommunernas lagstadgade uppgifter genom att kommunerna tilldelas landskapsandelar och komplettering av skatteinkomster.

4.1.5. Finansiella intäkter och kostnader

Beloppet består främst av ränteutgifter på lån och därtill hörande lånekostnader. Beloppet kan även innefatta inkomsträntor från skatteredovisningen, förseningsräntor på kommunens utestående fordringar samt vissa andra inkomsträntor.

4.1.6. Årsbidraget

Driftshushållningens överskott eller det s.k. årsbidraget är ett kommunalekonomiskt relationstal som beskriver kommunens egen finansieringsförmåga för investeringar. Årsbidraget utgör det mest centrala ekonomiska jämförelsetalet för kommuner och anger hur mycket som återstår för amorteringar och avskrivningar. Målsättningen för årsbidragets storlek är beroende på den enskilda kommunens finansieringsläge och investeringsbehov.

4.1.7. Avskrivningar och nedskrivningar

Utgör kostnaden för aktivering av kommunens anläggningstillgångar. Avskrivningarna återspeglar alltså den årliga förslitningen av kommunens tillgångar. Avskrivningarna följer en av kommunfullmäktige uppgjord plan.

4.1.8. Räkenskapsperiodens resultat

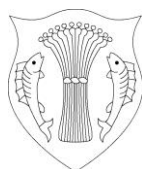
Anger resultatet före förändringar i avskrivningsdifferens, förändringar i reserver eller förändringar i fonder.

4.1.9. Ökning/minskning av reserver

Visar eventuella förändringar i reserver.

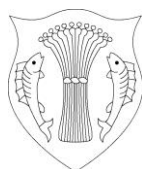
4.1.10. Över- eller underskott

Över- eller underskottet visar den uppskattade förändringen i kommunens eget kapital. Ett underskott minskar på kommunens eget kapital medan ett överskott ökar det egna kapitalet.



4.2. Resultaträkning

Resultaträkning	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
Verksamhetens intäkter	426 679,03	330 753,00	554 743,00	560 290,43	565 893,33
Verksamhetens kostnader	-2 989 708,48	-3 028 278,87	-3 233 193,88	-3 265 525,82	-3 298 181,08
Verksamhetsbidrag	-2 563 029,45	-2 697 525,87	-2 678 450,88	-2 705 235,39	-2 732 287,74
Förändring i %		5,25 %	-0,71 %	1,00 %	1,00 %
Skatteinkomster	1 684 456,26	1 601 000,00	1 592 000,00	1 592 000,00	1 592 000,00
Landskapsandelar	819 763,11	826 466,00	779 497,00	779 497,00	779 497,00
Finansiella intäkter och kostnader	-58 119,75	-115 360,83	-125 089,92	-125 089,92	-125 089,92
Årsbidrag	-116 929,83	-385 420,70	-432 043,80	-458 828,31	-485 880,66
Förändring i %		229,62 %	11,85 %	6,20 %	5,90 %
Avskrivningar och nedskrivningar	-166 566,56	-181 612,00	-164 818,00	-180 612,00	-180 612,00
Extra ordinära poster	50 233,64				
Räkenskapsperiodens resultat	-233 262,75	-567 032,70	-596 861,80	-639 440,31	-666 492,66
Ökning/minskning av reserver					
Räkenskapsperiodens över/underskott	-233 262,75	-567 032,70	-596 861,80	-639 440,31	-666 492,66
Budgerade över- och underskott år 2023-2025 sammanlagt:			-1 397 157,25		



4.3. Finansieringsanalys

Finansieringsanalys	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
Årsbidrag	-116 929,83	-385 420,70	-432 043,80	-458 828,31	-485 880,66
Extraordinära poster	50 233,64				
Korrektivposter till internt tillförda medel					
Investeringsutgifter	-639 972,71	-1 251 000,00	-105 000,00	-105 000,00	-40 000,00
Finansieringsandelar för investeringar		40 500,00			
Inkomster från överlåtelse av tillgångar bland bestående aktiva					
Verksamhetens och investeringarnas kassaflöde	-706 668,90	-1 595 920,70	-537 043,80	-563 828,31	-525 880,66
Ökning av utlåningen					
Minskning av utlåningen					
Ökning av långfristiga lån	470 798,02	988 000,00	105 000,00	105 000,00	40 000,00
Minskning av långfristiga lån	-97 703,50	-138 740,28	-127 495,74	-127 495,74	-127 495,74
Förändring av kortfristiga lån	36 886,98				
Förändring av lånebeståndet	409 981,50	849 259,72	-22 495,74	-22 495,74	-87 495,74
Förändring i eget kapital					
Förändring av förvaltad medel och kapital					
Förändring av omsättningstillg.					
Förändring av fordringar	13 998,49				
Förändring av räntefria skulder	29 753,58				
Förändring av likvida medel	-252 935,33	-746 660,98	-559 539,54	-586 324,05	-613 376,40
Kassamedel 1.1	414 604,33	161 669,00	-584 991,98	-1 144 531,52	-1 730 855,57
Kassamedel 31.12	161 669,00	-584 991,98	-1 144 531,52	-1 730 855,57	-2 344 231,97
Skuldbörda	1 968 000,00	2 817 135,73	2 794 639,99	2 772 144,25	2 684 648,51
Lån per invånare	5 377,00	7 697,00	7 614,82	7 553,53	7 315,12



4.4. Skattekalkyl

Skatteinkomster	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
A5100 SKATTEINKOMSTER					
5000 Kommunal inkomstskatt	1 546 890,11	1 480 000,00	1 456 000,00	1 456 000,00	1 456 000,00
5100 Fastighetsskatt	81 557,61	84 000,00	84 000,00	84 000,00	84 000,00
5200 Andel av samfundsskatt	47 881,42	30 000,00	44 000,00	44 000,00	44 000,00
5300 Källskatt	8 127,12	7 000,00	8 000,00	8 000,00	8 000,00
A5100 SKATTEINKOMSTER Summa	1 684 456,26	1 601 000,00	1 592 000,00	1 592 000,00	1 592 000,00

4.5. Landskapsandelar

Landskapsandelar och kompensationer	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
A5110 LANDSKAPSANDELAR O. KOMPENSATIONER					
5601 Landskapsandel barnomsorg	33 210,24	32 547,00	46 977,00	46 977,00	46 977,00
5602 Landskapsandel äldreomsorg	68 920,39	71 747,00	84 914,00	84 914,00	84 914,00
5604 Landskapsandel träningsundervisningen	38 058,15	39 785,00			
5700 Landskapsandel för grundskola	246 269,40	253 673,00	220 206,00	220 206,00	220 206,00
5716 Landskapsandelar för kultur	6 160,01	6 165,00	6 551,00	6 551,00	6 551,00
5900 Skattekomplettering	314 717,59	307 675,00	316 119,00	319 280,19	319 280,19
5912 Kompensation för resekostnadsavdrag	95 795,07	36 401,00	38 395,00	38 395,00	38 395,00
5913 Kompensation för grundavdrag		59 394,00	44 895,00	44 895,00	44 895,00
5914 Kompensation för samf. skatteint.	16 095,64	19 079,00	21 440,00	21 440,00	21 440,00
5990 Övriga kompensationer	536,62				
A5110 LANDSKAPSANDELAR O. KOMPENSATIONER Summa	819 763,11	826 466,00	779 497,00	782 658,19	782 658,19



5. KOMMUNFULLMÄKTIGES VISION OCH MÅLSÄTTNINGAR

5.1. Vision

Att ge kommuninvånarna en prisvärd relevant service av hög kvalitet. Lumparland fortsätter att existera som en självständig kommun och erbjuder när demokrati för invånarnas bästa.

5.2. Verksamhetsmål 2025

- Att se till att kommunens basservice (barnomsorg, skola och äldreomsorg) sköts så effektivt och förmånligt som möjligt i egen regi.

5.3. Verksamhetsmål 2026–2027

- Att utveckla servicen både självständigt och i samarbete med andra aktörer.

5.4. Åtgärder för att uppnå de uppställda målen

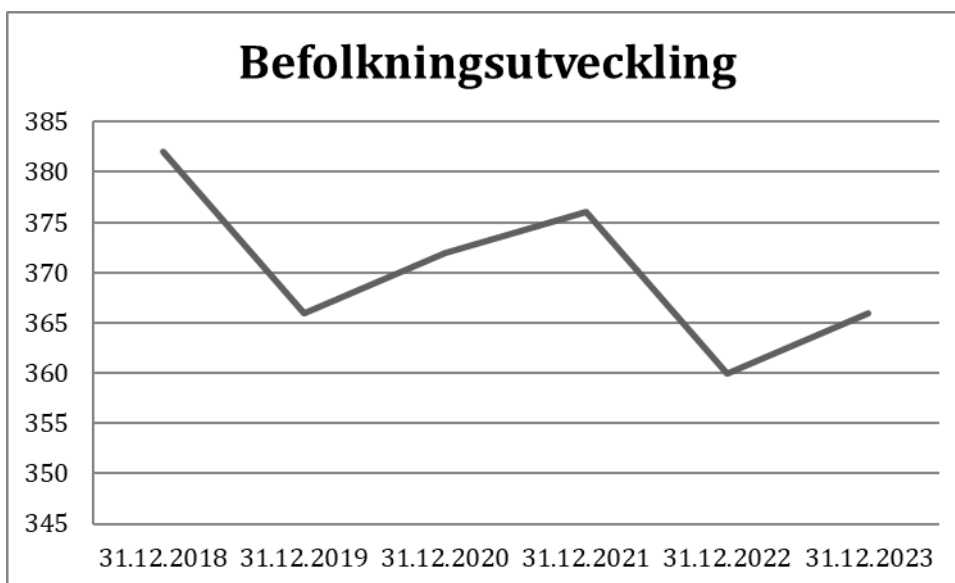
- Möjliggöra inflyttning genom att erbjuda bostäder och bostadstomter, vilket leder till högre skatteintäkter. Eventuella möjliga markköp utreds under år 2025.
- Effektivisera servicen inom ramen för en självständig kommun med hjälp av relevanta IKT-lösningar.



6. BUDGETFÖRUTSÄTTNINGAR

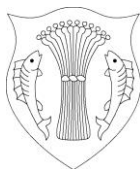
6.1. Befolkningsuppgifter

Befolkningen i kommunen har sedan 31.12.2017 minskat från 385 personer till 360 personer 31.12.2022. Den ekonomiska utvecklingen i kommunen är stram med hänsyn till de indikatorer som finns tillgängliga. Utmaningarna är främst befolkningsutvecklingen och befolkningsstrukturen med avseende på försörjningsbördan och den framtida ekonomiska utvecklingen i kommunen.



Ålder	31.12.2018	Andel	31.12.2019	Andel	31.12.2020	Andel	31.12.2021	Andel	31.12.2022	Andel	31.12.2023	Andel
0-14	60	15,19 %	53	14,48 %	55	14,78 %	57	15,16 %	46	12,78 %	47	12,84 %
15-64	216	54,68 %	207	56,56 %	215	57,80 %	212	56,38 %	209	58,06 %	211	57,65 %
65-	106	26,84 %	106	28,96 %	102	27,42 %	107	28,46 %	105	29,17 %	108	29,51 %
Totalt	395		366		372		376		360		366	

Ålder	Lumparland	Andel	Åland	Andel
0-14	47	12,84 %	4 871	15,95 %
15-64	211	57,65 %	18 286	59,87 %
65-	108	29,51 %	7 384	24,18 %
Totalt	366	100,00 %	30 541	100,00 %



6.2. Skattesatser

6.2.1. Inkomstskatten

Inkomstskattesatsen är 19,50 procent.

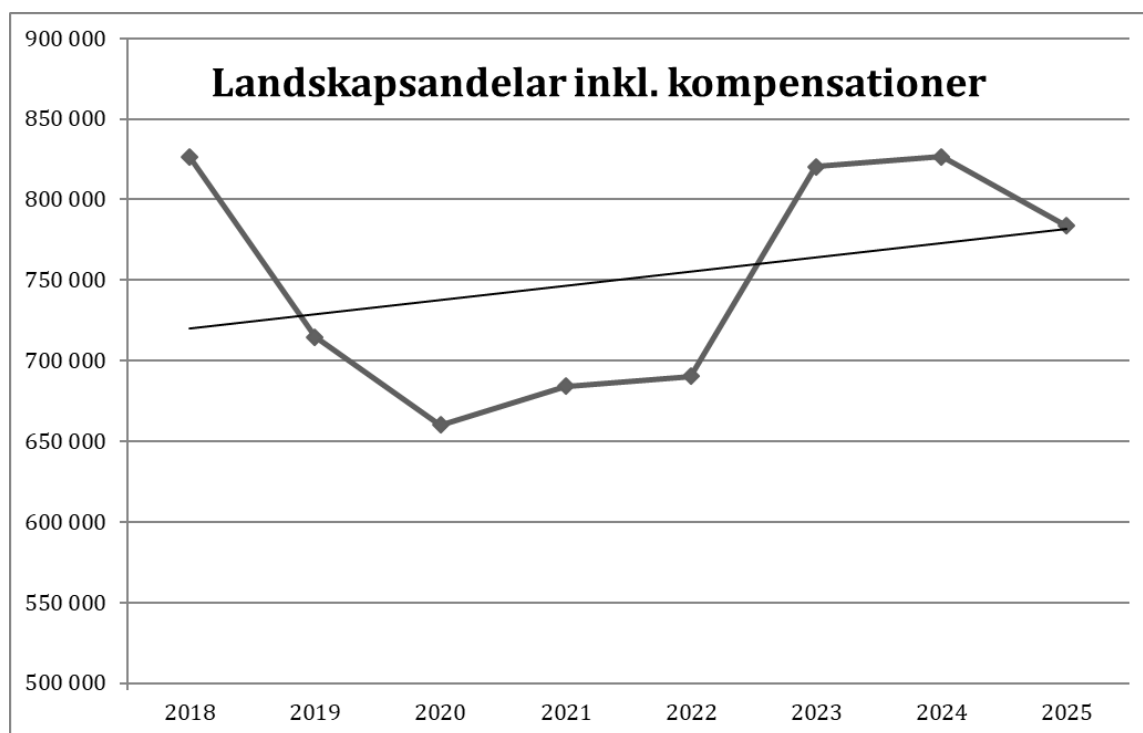
Inkomstskattesatsförändring	Uppskattad påverkan i euro
1 %	75 000
0,50 %	37 500
0,25 %	7 500

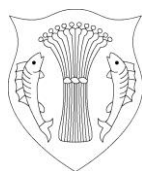
6.2.2. Fastighetsskatten

	2025
Allmän för byggnader	0,60 %
Allmän för markområden	0,60 %
Övriga bostadsbyggnader	0,90 %
Allmännyttiga samfund	0,00 %
Obebyggd byggplats	1,00 %
Kraftverk	0,60 %

6.3. Landskapsandelar

Landskapsandelarna inklusive kompensationer för 2025 förväntas vara 779 497 euro.





6.4. Kommunens skuldsättning

Under året förväntas skuldsättningen att minska med 22 495,74 euro. Under året planeras amorteringar på 127 495,74 euro. (kommunen inväntar beslut om amorteringsfrihet)

6.5. Miljönyckeltal

Prestationer	Bokslut 2022	Budget 2023	Bokslut 2023
Medel för lokalt miljöarbete i Lumparland €	1 331	1 600	982
Elektricitetskonsumtion, CO₂ utsläpp			
Samtliga kostnadsställen med elkonsumtion använder 100 % vindenergi	0	-	0
Bränsle, CO₂ utsläpp			
Eldningsolja, 1 ton	3,4	-	3,6
Vatten och avlopp			
Administration, m ³	24	-	22
Omsorg, m ³	579	-	555
Skola, m ³	250	-	217
Daghem, m ³	208	-	91
Boende, m ³	727	-	814
Vatten och avlopp totalt, m³	1788	-	1699

Miljönyckeltalen tas fram av byggnads- och miljönämnden vid uppgörandet av bokslutet. Eventuella målsättningar kring miljön ställs antingen upp av berörd nämnd eller kommunfullmäktige i budget.



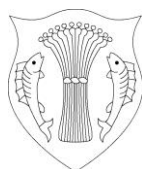
6.6. Personal

Inom daghemmet finns budgeterat för tillfällig barnskötare på heltid för hela året.

I skolan budgeteras för en ytterligare assistent och en till timlärare för att från höstterminen 2025 ha tre klasser i skolan.

Inom äldreomsorgen har budgeterats för en vikariepool på 0,50 årsverken för att säkra upp bemanningen under ordinarie personals frånvaro, i likhet med föregående år.

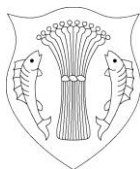
Biblioteket slutar ha öppet vid kortare ledigheter för bibliotekssekreteraren, men kommer fortsättningsvis ha semestervikarie under sommaren.



Budget 2025 och ekonomiplan 2026–27 för Lumparlands kommun

	Budget 2024	Budget 2025
Centralförvaltningen	2,60	2,60
Kommundirektör	1,00	1,00
Ekonomichef	0,80	0,80
Byråsekreterare	0,80	0,80
Äldreomsorgsförvaltningen	12,73	12,15
Äldreomsorgschef*	0,30	0,30
Administratör*	0,30	0,30
Ledande närvårdare	1,00	1,00
Ställföreträdande ledande närvårdare	1,00	1,00
Närvårdare	6,87	6,35
"Pool"-resurs	0,50	0,50
Kock	0,80	0,80
Vikarier	1,96	1,90
Bildningsförvaltningen	10,45	11,53
<u>Barnomsorg</u>	<u>4,73</u>	<u>5,35</u>
Barnomsorgsledare*	0,13	0,13
Administratör*	0,13	0,13
Daghemsföreståndare	1,00	1,00
Lärare inom barnomsorg	1,00	1,00
Barnskötare	1,20	1,98
Lokalvårdare/köksbiträde	0,80	0,80
Vikarier	0,47	0,31
<u>Grundskola</u>	<u>5,72</u>	<u>6,18</u>
Skolföreståndare	1,00	1,00
Klasslärare i huvudsyssla	0,93	1,00
Timlärare i huvudsyssla	0,95	1,28
FBU-lärare	0,11	0,00
Assistent	0,54	0,77
Kock	1,00	1,00
Lokalvårdare/köksbiträde	1,00	1,00
Vikarier	0,19	0,13
Kultur-och fritidsförvaltningen	0,79	0,76
Bibliotek	0,50	0,50
Biblioteksvikarier	0,17	0,10
Ungdomsarbete	0,12	0,16
Byggnads- och miljönämnden*	0,35	0,20
Tekniska nämnden*	1,57	1,30
Brand- och räddningsväsendet*	0,05	0,02
Totalt	28,54	28,56

*Lumparlands del av den totala personalen



6.6.1. Personalkostnader

De totala personalkostnaderna ökar från 1 347 560,60 euro 2024 till 1 548 301,40 euro 2025. Anledningen är kollektivavtalsenliga löneförhöjningar, höjning av KEVAS pensionsavgift med 20 000 euro, En ytterligare timplärare i skolan, en assistent till i skolan, en tillfällig barnskötare på 100 procent istället för 80 procent samt att ungdomsgården är öppen två dagar i veckan istället för en dag.

6.6.2. Arbetshälsa

Kommunen har den lagstadgade företagshälsovården i vilken ingår arbetsplatsbesök och hälsoundersökningar samt besök till läkare och arbetsfysioterapeut.

6.6.2.1. Friskvård

Lumparlands kommun erbjuder sina anställda 200 euro per år i friskvårdskuponger genom Friskvård.ax.



7. DRIFTSEKONOMIN I DETALJ

7.1. Centralförvaltningen

C100 Allmän förvaltning		Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
<input checked="" type="checkbox"/> C110	Val	-1 013,46	-1 837,00	-356,80		
	1101 Kommunal- och lagtingsval	-743,13	-65,40	-6,50		
	1102 Riksdagsval	-257,73	-58,80	-6,50		
	1103 Presidentval	-6,30	-1 111,40	-227,00		
	1104 EU-val	-6,30	-601,40	-116,80		
<input checked="" type="checkbox"/> C120	Allmän förvaltning	-2 586 449,65	-2 737 829,90	-2 628 882,48		
	1201 Revision	-2 918,59	-5 886,50	-5 904,50		
	1202 Kommunfullmäktige	-3 134,03	-4 317,30	-4 359,00		
	1203 Kommunstyrelsen	-13 271,59	-9 714,40	-7 899,10		
	1204 Kommunkansliet	-2 184 449,68	-2 322 247,90	-2 261 899,08		
	1205 Allmän förvaltning	-13 319,23	-10 186,50	-10 913,70		
	1206 Företagshälsovård	-1 113,01	-1 000,00	-1 000,00		
	1207 Ålands skattebyrå	-4 035,28	-8 000,00	-4 100,00		
	1208 Lumparlands Info	-2 403,24	-2 430,30	-2 517,10		
Totalsumma		-2 596 588,11	-2 756 199,90	-2 632 339,28	-2 658 871,67	-2 688 530,39

Anslagsansvarig

Kommundirektören.

Centralförvaltningens interna uppgift är att sköta administrationen för kommunfullmäktige, kommunstyrelsen och av kommunstyrelsen tillsatta kommittéer samt att bistå den övriga förvaltningen med sakkunskap och ekonomisk rådgivning samt koordinera kommunens budget och bokslut, sköta bokföringen, löneutbetalningen och faktureringen. Centralförvaltningens externa uppgift är att fungera som ansikte utåt, att tillhandahålla information och basfakta om kommunen samt att informera om aktuella frågor av lokalt intresse, vilka på ett eller annat sätt berör kommuninvånarna.

7.1.1. Kommunfullmäktige

Kommunens högsta beslutanderätt tillkommer kommunfullmäktige. Fullmäktige godkänner budgeten och ekonomiplanen, fastställer skattesatsen och kommunens avgifter, beslutar om långfristiga lån m.m. Resultatenheten omfattar främst anslag för mötesarvoden åt kommunens förtroendevalda och tjänsteinnehavare för fullmäktiges sammanträden samt andra därtill hörande kostnader.

7.1.2. Kommunstyrelsen

Kommunstyrelsen ansvarar bl.a. för kommunens förvaltning och ekonomi, bevakar kommunens intressen, företräder kommunen och för kommunens talan, om inte fullmäktige eller speciallagstiftning påtalar annat.



7.1.3. Revision

För granskning av förvaltningen och räkenskaperna, som utförs för varje löpande räkenskapsår, väljer kommunfullmäktige efter nyval för sin mandatperiod revisorer och för dem en personlig ersättare och utser en som fungerar som yrkesrevisor.

7.1.4. Val

Inga val planeras under år 2025.

7.1.5. Kommunkansliet

I anslaget ingår löner till kommunkansliet personal, post- och teletjänster och materialinköp m.m. Följande merkostnader uppkommer:

- Löneförhöjningar om cirka 3 300 euro.
- Kevas utjämningsavgift har höjts kraftigt pga välfärdsreformen, merkostnad 6 414 euro.

Ordinarie personal	Budget 2023	Budget 2024
Kommundirektör	1,00	1,00
Ekonomichef	0,80	0,80
Byråsekreterare	0,80	0,80
Totalt	2,60	2,60

7.1.6. Allmän förvaltning

I anslaget ingår förvaltningsgemensamma utgifter såsom medlemsavgifter och utbildning som är verksamhetsöverskridande.

7.1.7. Företagshälsovården

Omfattar den lagstadgade företagshälsovården. De lagstadgade företagshälsovårdstjänsterna köps av Cityläkarna Ab.

7.1.8. Beskattning

Omfattar kommunens andel av de kostnader som Skatteförvaltningen uppbär för administration av skatteintäkter.

7.1.9. Lumparlands info

Under detta moment upptas anslag för kommunens infoblad, vilket utkommer elva gånger per år med dubbelnummer för juni-juli samt anslag för skötseln av kommunens webbplats på internet. Kommunens infoblad sköts av ekonomichefen och webbplatsen av byråsekreteraren. Dessa medier är centrala för kommunens informationsverksamhet.



7.2. Lantbruksnämnden

C101 Lantbruk	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
1210 Lantbruksnämnden	-7 271,00	-10 821,00	-7 000,00		
Totalsumma	-7 271,00	-10 821,00	-7 000,00	-7 070,00	-7 140,70

Anslagsansvarig

Lantbrukssekreteraren.

Lantbruksnämnden handhar lantbruksförvaltningen enligt landskapslagen om lantbruksnämnder (1998:85) och landskapslagen om främjande av gårdsbruk (1998:54), lagen om förvaltningen av landsbygdsnärningar i kommunerna (FFS 1558/1991) samt livsmedelsverkets direktiv angående administrationen av frågor rörande understöd till lantbruket.

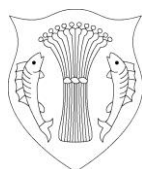
Lantbruksnämnden är gemensam med Hammarlands, Eckerö och Föglö kommuner där Hammarlands kommun är huvudman för samarbetet.

Målsättning

Att sköta de uppgifter inom lantbruksförvaltningen som ålagts kommunerna.

Allmänt	Bokslut 2023	Budget 2024	Budget 2025
Antal sammanträden	2	2	2
Lumparlands andel av lantbrukssekreterare % av heltid	12,5 %	12,5 %	12,5 %
Gårdar som ansöker om stöd	7	7	7

Ansökningar	Bokslut 2023	Budget 2024	Budget 2025
Huvudstödsansökan totalt st	7	8	7
Höstanmälan totalt st	7	7	7
Stödbeslut totalt	31	31	31
pappersblanketter totalt	8	6	0
anmälan om deltagande	0	8	0
skiftesann./-ändringar	33	3	33
Beviljade lantbr.stöd totalt inkl. stöd från ÅLR	488 750		
Kostnad per gård			1 117



7.3. Samordnad socialtjänst (Kommunernas socialtjänst k.f.)

C200 Socialsektorn	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
C210 Socialförvaltning (övr. socialv.)	-337 853,86	-332 965,95	-372 000,00		
2102 Socialkansliet	,45	-555,75			
2104 Samordnad socialtjänst (KST)	-337 854,31	-332 410,20	-372 000,00		
Totalsumma	-337 853,86	-332 965,95	-372 000,00	-375 720,00	-379 477,20

Anslagsansvarig

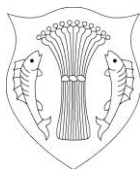
Kommundirektören.

I enlighet med landskapslagen om en kommunalt samordnad socialtjänst (2016:2) har Kommunernas socialtjänst k.f. (KST) ansvaret för förverkligandet av socialvården exklusive äldreomsorgen på Åland.

Kommunalförbundets verksamhet omfattar all den socialvård som enligt lag ankommer kommunerna i enlighet med 1 § i landskapslagen om kommunalt samordnad socialtjänst och utgör ett för landskapet Åland gemensamt socialvårdsområde i enlighet med 3 § 1 mom. i nämnda lag. I enlighet med det grundavtal som kommunerna godkänt ska förbundet främja invånarnas hälsa och välfärd och säkerställa att de socialvårdstjänster som var och en har rätt till finns att tillgå för samtliga invånare i socialvårdsområdet.

Främjandet av invånarnas hälsa och välfärd och verkställandet av kommunalförbundets verksamhet sker i samarbete med kommuner och andra myndigheter. Vidare ska verksamheten sträva efter en likvärdig service i alla medlemskommuner, en effektiv användning av resurserna, en samlad kompetens och hög specialisering inom personalen, en hög integritet, en stark anonymitet och ett gott rättsskydd. Det grundläggande uppdraget för socialvården är att upprätthålla individers funktionsförmåga så att alla har möjlighet att fungera som fullvärdiga medlemmar i samhället.

Enligt grundavtalet ska finansiering av kommunalförbundet ske solidariskt genom en fördelning av kostnaderna baserad på befolkningsmängd och skattekraft.



7.4. Äldreomsorgsförvaltningen

C230 Omsorg om äldre	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
C230 Omsorg om äldre	-702 481,74	-827 031,78	-943 080,78		
C234 Äldreomsorgsledning	-29 638,73	-30 078,00	-30 085,00		
2313 Äldreomsorgsledning	-29 638,73	-30 078,00	-30 085,00		
C231 Vård på åldringshem	-29 726,57	-21 150,00	-30 000,00		
2311 Oasen	-29 726,57	-21 150,00	-30 000,00		
C233 Hemtjänst	-643 116,44	-775 803,78	-882 995,78		
2331 Hemvård	-51 299,56	-59 029,05	-72 179,48		
2334 Kapellhagens serviceboende	-451 145,51	-566 958,23	-605 699,80		
2336 Serviceboende i annan kommun	-130 670,00	-130 670,00	-176 300,00		
2337 Äldrerådet	-1 098,31	-1 740,00	-1 740,00		
2423 Närståendevård	-8 903,06	-17 406,50	-27 076,50		
Totalsumma	-702 481,74	-827 031,78	-943 080,78	-952 511,59	-962 036,70

Anslagsansvarig

Äldreomsorgschefen.

Äldreomsorgsledningen sköts från och med 1.1.2021 gemensamt med Lemland i enlighet med ett samarbetsavtal kommunerna emellan.

Förvaltningen omfattar hemvårdshjälp, effektiverade serviceboende (ESB) Kapellhagen, trygghetstelefon, närståendevård samt institutionsvård. Hemservicearbetet består av olika hemservice- och stödtjänster till de boende på ESB Kapellhagen samt till övriga kommuninvånare som har behov av denna service.

Målsättning

- Införa vård- och informationssystemet VIS samt delta i förstudien för VIVA.

7.4.1. ESB Kapellhagen

Kapellhagen är ett serviceboende med heldygnsomsorg sedan 2015. Verksamheten består av vård, omsorg, tillsyn och sysselsättning för de boende samt vanlig hemservice. På Kapellhagen finns det 11 permanenta platser och en avlastningsplats.

Ordinarie personal	Budget 2024	Budget 2025
Ledande närvårdare	1,00	1,00
Ställföreträdande ledande närvårdare	1,00	1,00
Närvårdare	6,87	6,37
Kock	0,80	0,80
"Pool"-resurs	0,50	0,50
Totalt	10,17	9,65



Målsättning

- Fortsätta det aktiva arbetet med att möjliggöra för flera att bo hemma så länge som möjligt med stöd av hemservice och förebyggande åtgärder.

7.4.2. Hemservice

Behovet av hemservice utanför Kapellhagen beräknas motsvara 10 % av personalens arbetstid. Hemservicen strävar till att genom god omsorg arbeta förebyggande och i samverkan med andra som t.ex. hemsjukvården, närståendevården och församlingen för att gynna äldre personers möjligheter att bo hemma.

7.4.3. Oasen boende- och vårdcenter k.f.

Kommunen äger två platser på Oasen boende- och vårdcenter. För platserna betalas en grundavgift oavsett om kommunen nyttjar platserna eller ej. Ifall kommunen använder platsen betalas utöver grundavgiften också en dygnsavgift. Om någon annan kommun utnyttjar Lumparlands platser betalas ingen grundavgift.



7.5. Bildningsförvaltningen

C300 Bildningsförvaltningen	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
C220 Barnomsorg	-198 862,54	-266 087,08	-275 095,62		
C224 Barnomsorgsledning	-16 253,15	-10 026,00	-16 176,00		
2213 Barnomsorgsledning	-16 253,15	-10 026,00	-16 176,00		
C221 Barnomsorg i daghem	-157 118,31	-212 651,08	-234 619,62		
+ 2211 Daghemmet Videungen och Myrstacken	-157 118,31	-212 651,08	-234 619,62		
C222 Familjedagvård för barn	-3,35				
+ 2250 Familjedagvård	-3,35				
C223 Övrig barndagvård	-25 490,73	-43 410,00	-24 300,00		
+ 2221 Hemvårdsstöd för barn	-25 490,73	-43 410,00	-24 300,00		
C320 Grundskola	-708 770,22	-645 276,44	-615 898,10		
3201 Lågstadiet	-332 895,79	-335 364,44	-372 579,10		
3202 Högstadiet	-283 523,06	-257 174,00	-243 319,00		
+ 3203 Träningssundervisningen	-46 853,31	-24 738,00			
+ 3205 Lågstadieelever i andra kommuner	-45 498,06	-28 000,00			
Totalsumma	-907 632,76	-911 363,52	-890 993,72	-899 903,66	-908 902,69

7.5.1. Bildningsförvaltningen

Anslagsansvarig

Utbildningschefen.

Bildningsförvaltningen ska planera utveckla, genomföra, samordna, uppfölja och utvärdera utbildningsverksamheten i kommunen. Bildningsförvaltningen ska ansvara för att landskapslagen om barnomsorg och grundskola följs och att den verksamhet som regleras i lagen erbjuds i kommunen.

Bildningsförvaltningen ska då den organiserar barnomsorgen och grundskoleutbildningen samarbeta mot de instanser som ansvarar för idrott och kultur, barnskydd och annan socialvård, rådgivningsverksamhet och övrig hälso- och sjukvård samt andra kommuners utbildningsverksamhet och aktörer.

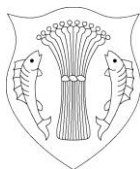
7.5.2. Barnomsorg

Barnomsorgsledningen sköts från och med 1.1.2021 gemensamt med Lemland i enlighet med ett samarbetsavtal kommunerna emellan. Speciallärartjänster inom barnomsorgen köps genom avtal av Lemland.

Den nya lagen om barnomsorg och grundskola (2020:32) samt den nya läroplanen för barnomsorgen påverkar fortsättningsvis barnomsorgens verksamhet. Den nya läroplanen behöver implementeras i enlighet med Ålands landskapsregerings reviderade plan för implementering 2024–2026 genom tillräcklig utbildning och handledning för barnomsorgspersonalen.

7.5.2.1. Barnomsorg i daghem

Prognosmässigt kommer barnantalet att öka vid daghemmet Videungen under 2025, då barnantalet i kommunen har ökat från 2024. Enligt statistik från ÅSUB per 31.12.2023



finns det 17 barn i åldern 1–6 år i kommunen. Behovet av fritidshemsplatser inför höstterminen 2025 beräknas även det öka, då det just nu (per 30.9.2024) är 8 förskolebarn på daghemmet.

Kommunen säljer platser till andra kommuner i den mån platser efterfrågas.

En tillfällig barnskötare behövs på daghemmet för att möta upp behovet av att barngruppen blivit större, främst för åldersgruppen 0–2 år samt inför hösten 2025 då antalet fritidshemsbarn beräknas öka.

Ordinarie personal	Budget 2024	Budget 2025
Daghemsföreståndare	1,00	1,00
Lärare inom barnomsorg	1,00	1,00
Barnskötare	1,20	1,98
Lokalvårdare/köksbiträde	0,80	0,80
Totalt	4,00	4,78

7.5.2.2. Hemvårdsstöd för barn

Vårdnadshavare för barn under 3 år som inte utnyttjar av kommunen bekostad barnomsorg har enligt lag rätt att få stöd för vård av barn i hemmet. Under 2025 är det en minskning av hemvårdsstöddagare i kommunen.

7.5.3. Lumparlands skola

Anslagsansvarig
Skolföreståndaren.

I skolan bedrivs grundskoleundervisning för barn i åldrarna 7-12 år. Distriktet omfattar årskurs 1-6 i kommunen. Ansvarig för verksamheten är kommunstyrelsen. Skolans föreståndare ansvarar för att verksamheten bedrivs i enlighet med skolans styrdokument och kommunstyrelsens beslut och anvisningar.

Målsättning

- Ge eleverna en trygg och kunskapsutvecklande miljö som skapar goda förutsättningar för framtida studier
- Bibehålla den goda stämningen i skolan och förstärka "vi"-känslan med tanke på litenheten
- Fortsätta ge eleverna en utbildning av hög kvalitet vilket gör det möjligt med hjälp av vuxentätheten som finns i skolan



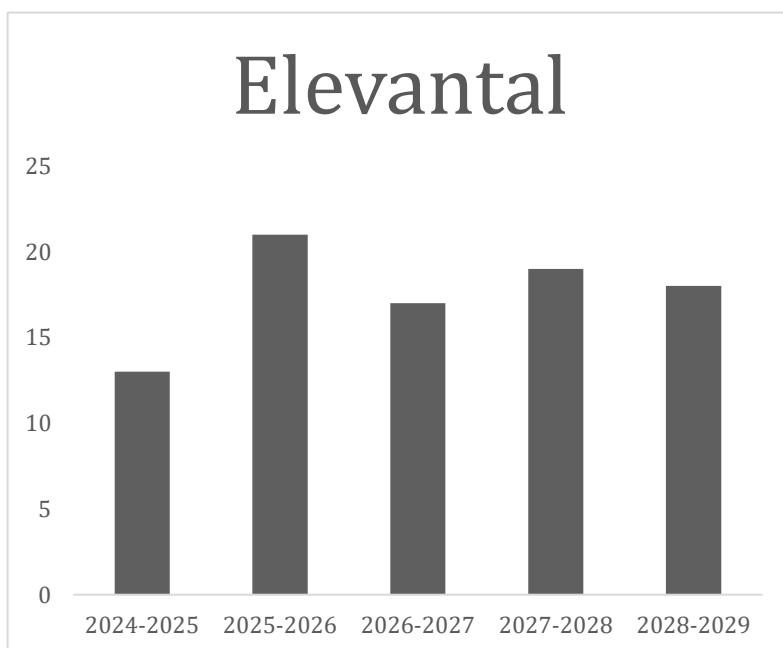
Klassorganisation	1.8.2024	Klassorganisation	1.8.2025
Klass	Antal elever	Klass	Antal elever
Åk 1-3	2+3+1	Åk 1	8
Åk 4-5	1+6	Åk 2-4	2+3+1
Totalt	13	Åk 5-6	1+6
		Totalt	21

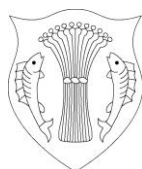
7.5.3.1. Personal

Ordinarie personal	1.8.2024	1.1.2025
Klass; timlärare och skolföreståndare	3	3,67
Elevassistent	0,54	1,09
Kanslipersonal	0	0
Kökspersonal	1	1
Städ-köksbiträde	1	1
Fastighetspersonal*	0	0

*Fastighetspersonal är ett samarbete mellan Lumparlands kommun och Lemlands kommun.

7.5.3.2. Elevantal





7.5.3.3. Timresursen

Begreppet timresurs är ett mått på antalet lärartimmar per vecka. Lumparlands skolas totala timresurs är enligt följande:

Timresurs fr.o.m. 1.8.2025	Antal lärartimmar	Lärartimmar per elev
Timresurs för allmän-undervisning (Au) på kommunens bekostnad	74	3,52
Timresurs för AU bekostad av SÅUD (språk, musik m.m)	0,00	0,00
Övrig timresurs på kommunens bekostnad	3,00	0,14
Special-undervisning på kommunens bekostnad	6,00	0,29
Special-undervisning bekostad av SÅHD	0,00	0,00
Totalt	83,00	3,95

7.5.3.4. Prestationstal

	2024	2025	Skillnad
Elever från Lumparland i Lumparlands skola	11,50	15,00	3,50
Elever från annan kommun/Ängö-Bussö Vårdö Kommun	1,00	2,00	1,00
Elever från Lu i annan kommun	0,50	0,00	-0,50
Antal elever i skolan	12,50	17,00	4,50
Elever i KHS	12,00	10,50	-1,50
Elever i träningsundervisningen	1,00	0,00	-1,00
Summa elever från Lumparland	25,00	25,50	0,50
Antal undervtim/vecka	66,00	74,50	8,50
Undervtim/elev	5,28	4,38	-0,90
Antal anställda totalt	5,54	6,05	0,51
Klass-, timplärare och skolföreståndare	3,00	3,28	0,28
Elevassistent	0,54	0,77	0,23
Kanslipersonal	0,00	0,00	0,00
Kökspersonal	1,00	1,00	0,00
Städ-köksbiträde	1,00	1,00	0
Fastighetspersonal	0	0	0,00
Kvm	740	740	0,00
Kvm/elev	59,20	43,53	-15,67
Elever som får skolskj.	4	6	2,00
Skjuts %	32 %	35 %	3,00 %



7.5.4. Kyrkby högstadieskola (KHS) och träningsundervisningen

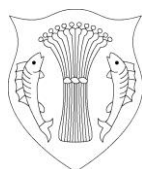
Lumparlands elever i årskurs 7-9 fullgör sin läroplikt i Kyrkby högstadieskola (KHS) i Jomala. Verksamheten sker inom ramen för SÅUD. Under 2025 beräknas 13 elever från Lumparland gå i KHS. Ingen elev från Lumparland beräknas gå i träningsundervisningen under 2025. En om- och tillbyggnad av KHS pågår och beräknas stå klar i december 2025.

7.5.5. Hemundervisning

Tidigare år har hemundervisningstillsynen enligt landskapslagen (2020:32) om barnomsorg och grundskola skett i egen regi genomförd av lärare i Lumparlands skola. Från och med 1.1.2024 köper Lumparlands kommun hemundervisningstillsyn av Mariehamns stad.

7.5.6. Ekonomiplan 2026–2027

I KHS förväntas antalet elever från Lumparland uppgå till 9,5 elever under år 2026 och 7,5 elever under år 2027. I träningsundervisningen förväntas ingen elev från Lumparland vara inskriven under år 2026 och 2027.

**7.6. Kultur- och fritidsförvaltningen**

C400 Kultur- och fritidsförvaltningen	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
C410 Kultur och fritid	-3 179,51	-33 518,60	-33 971,40		
4102 Biblioteket	-3 179,51	-33 518,60	-33 971,40		
C420 Idrott och friluftsliv	-1 574,56	-2 19,60	-1 103,00		
4201 Idrott och friluftsliv	-1 574,56	-2 19,60	-1 103,00		
C430 Ungdomsväsendet	-2 450,53	-8 672,52	-8 892,70		
4301 Ungdomsarbete	-2 450,53	-8 672,52	-8 892,70		
C440 Övrig kulturverksamhet	-6 061,07	-8 242,00	-6 938,00		
4401 Allmän kulturverksamhet	-6 061,07	-8 242,00	-6 938,00		
C450 Medborgarinstitutet	-6 868,39	-7 900,00	-6 000,00		
4501 Medborgarinstitutet	-6 868,39	-7 900,00	-6 000,00		
Totalsumma	-48 748,06	-58 552,72	-56 905,10	-57 474,15	-58 048,89

C400 Kultur- och fritidssektorn	Bokslut 2022	Budget 2023	Budget 2024
Extern	-48 309,52	-55 767,00	-57 809,90
Intern	-23 014,55	-43 220,08	-38 233,94
Totalsumma	-71 324,07	-98 987,08	-96 043,84

Anslagsansvarig

Bibliotekssekreteraren.

Kultur- och fritidsförvaltningen ansvarar för kommunens biblioteks-, fritids-, ungdoms- och kulturväsende. Förvaltningen handhar även frågor gällande medborgarinstitutet (Medis) och turism.

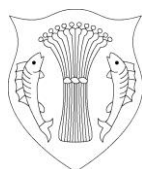
Den allmänna kulturverksamhetens huvuduppgift är att ordna kulturell verksamhet. Ungdomsarbetets uppgift är att ordna ungdomsverksamhet. Till idrotts- och friluftslivsverksamheten hör att möjliggöra juniorverksamhet och att ansvara för underhållet av motionsbanan. Kultur- och fritidsförvaltningen föreslår fördelning av föreningsbidrag. Biblioteket verkar som skol- och kommunbibliotek. Medborgarinstitutets uppgift är att erbjuda vuxna i Lumparland möjlighet till allmänbildande utbildning och meningsfull fritidssysselsättning.

Ordinarie personal	Budget 2024	Budget 2025
Bibliotekssekreterare	0,50	0,50
Ungdomsgårdsledare	0,12	0,16
Totalt	0,62	0,66

Målsättningar

Fortsatt arbete med att ha ett välfungerande kommunbibliotek i närområdet, ett bibliotek som även fungerar som ett skolbibliotek i direkt anslutning till skolan. Invånarna i kommunen ska kunna erbjudas meningsfulla fritidsaktiviteter i sin hemkommun, kursmöjligheter via Medis kursverksamhet och genom föreningsbidrag till lokala föreningar för att stöda ett blomstrande föreningsliv.

Fortsätta arbeta för att barnen och ungdomarna i Lumparland har en meningsfull fritid genom att ge föreningsbidrag till föreningar som ordnar aktiviteter för barn och ungdomar, genom att barnen i Lumparland ges möjlighet att delta i de fritidsaktiviteter som ar-



rangeras av Fritidsledarna i Lemland, men också genom att de ges möjlighet att delta i Stallets och Uncans fritidsaktiviteter i Mariehamn.

7.6.1. Föreningsbidrag

Förening	Andel av kostnader	Andel av aktiva medlemmar	Andel av totala medlemmar	Andel av aktiviteter	Andel av medeltal besökare	Belopp	Summa att fördela
Föreningen Folkhälsan i L.	46 %	57 %	51 %	29 %	3 %	741	
Lumparlands Ungdomsförening r.f.	11 %	9 %	15 %	10 %	50 %	381	2000
Nybondsi Krogstad r.f.	40 %	10 %	24 %	31 %	44 %	597	
Svinö Byalag	3 %	24 %	11 %	31 %	2 %	282	

7.6.2. Projektbidrag

Inga ansökningar om projektbidrag har inkommit.

7.6.3. Övriga bidragsansökningar

7.6.3.1. Ålands 4H-distrikt r.f.

Lumparlands kommun har som praxis att till Ålands 4H-distrikt r.f. bevilja bidrag om 5 euro per medlem som har Lumparlands kommun som hemkommun. Föreningen har 17 medlemmar med Lumparlands kommun som hemkommun.

85 euro beviljas (4740 4301) Ungdomsarbete.

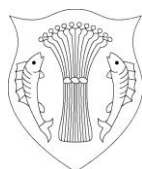
7.6.3.2. Föreningen Norden på Åland r.f.

Ansöker om 50 cent per invånare eller ett fast bidrag.

Ansökan avslås på grund av att föreningen inte har Lumparlands kommun som hemort.

7.6.4. Ekonomiplan 2026–2027

Under ekonomiplanepreioden hoppas förvaltningen ordna aktiviteter kring bibliotekets 100-årsfirande under 2026.



7.7. Byggnads- och miljönämnden

C500 Byggnadssektorn	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
C510 Byggnads förvaltning	-152,27	-104,00	-20 539,00		
+ 5103 Byggnads- och miljönämnden			-3 000,00		
+ 5105 Byggnads- och miljökansliet	-152,27	-104,00	-17 539,00		
C520 Byggnadstillsyn	-12 644,14	-14 224,00	1 150,00		
+ 5201 Byggnadsinspektionen	-12 644,14	-14 224,00	1 150,00		
C525 Samhälls planering	-2 483,83	-3 603,00	-1 550,00		
+ 1209 Planläggning	-2 483,83	-3 603,00	-1 550,00		
C530 Miljö vård	-2 974,00	-3 607,00	-1 350,00		
+ 5302 Övrig miljö verksamhet	-2 974,00	-3 607,00	-1 350,00		
C535 Avfallshandling	-5 982,85	-4 121,00	-2 750,00		
+ 5952 Krogstad avfallsdeponi	-5 982,85	-4 121,00	-2 750,00		
Totalsumma	-24 237,09	-25 659,00	-25 039,00	-25 289,39	-25 542,28

Anslagsansvarig

Byggnads- och miljöinspektören.

Byggnads- och miljösektorns verksamhetsområde omfattar i huvudsak byggnadstillsyn, planläggning, avfallshandling, jord- och skogsbruk samt miljövärd.

7.7.1.1. Verksamhets- och volymförändringar 2025

-

7.7.1.2. Verksamhetsmål 2025

Mål:	Metod:
1. Revidering av Lumparlands byggnadsordning	1. intern process
2. Revidering av detaljplan i Långnäs	2. extern/intern process

7.7.1.3. Verksamhetsmål 2026–2027

Mål:	Metod:
1. Revidera kommunöversikten	1. Intern process

7.7.2. Byggnads- och miljönämnd

Verksamheten omfattar nämndens löpande arbete. Nämnden planerar sammanträda sex gånger under året.

7.7.3. Byggnads- och miljökansliet

Verksamheten omfattar kanslifunktionen inom byggnads- och miljösektorn i Lumparland. Kanslifunktionen köps i huvudsak utifrån. Budget, bokslut samt övrig ekonomi sköts av Lumparland.



7.7.4. **Byggnadstillsyn**

Resultatenheten omfattar byggnadstillsynen i Lumparland. Verksamheten omfattar i praktiken beredning och uppföljning av bygglov, avloppstillstånd, adressregistret och dylikt. Därtill fakturering av tillståndsavgifter enligt gällande taxor samt upprätthållande och rapportering av byggnadsdata.

NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Tillståndsärenden Lumparland (st)	21	25	25
Avgifternas täckningsgrad Lumparland	46,0%	36,0%	21,0%

7.7.5. **Planläggning**

Resultatenheten omfattar detalj- och generalplanering samt kommunöversikterna i Lumparland. Nämnden samarbetar med landskapsregeringen, planläggare, kartläggare och andra experter vid behov.

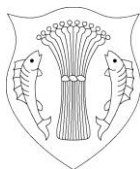
7.7.6. **Miljövård**

Resultatenheten består av anslag för miljöarbete i Lemland och Lumparland. Visionen för verksamheten är en hållbar samhällsutveckling, ren och utsläppsfri miljö samt att alla avloppsanläggningar i Lumparland är miljömässigt hållbara.

Verksamheten består också av information samt uppföljning av funktionen hos två våtmarker vid Kapellviken.

7.7.7. **Krogstad avfallsdeponi**

Verksamheten har gällande miljötillstånd. I enlighet med tillståndet ska t ex vattenprover tas kontinuerligt. Resultaten delges ÅMHM.



7.8. Tekniska nämnden

C501 Tekniska sektorn	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
[-] C511 Teknisk förvaltning				-31 100,00	
+ 5102 Tekniska nämnden					
+ 5104 Tekniska kansliet				-31 100,00	
[-] C540 Trafikleder	-54 821,99	-56 521,00	-34 300,00		
+ 5401 Kommunalvägar	-14 905,76	-11 987,00	-13 500,00		
+ 5402 Bygdevägar	-3 327,83	-2 123,00			
+ 5403 Cykel- och gångvägar	-6 698,36	-7 391,00	-8 000,00		
+ 5404 Snöplogning	-2 540,68	-4 998,00	-3 100,00		
+ 5450 Bostadsgator	-11 389,56	-11 619,00	-2 500,00		
+ 5451 Vägbesynning	-13 940,80	-15 134,00	-6 500,00		
+ 5452 Rastplats Lumparsund	-1 883,00	-2 589,00	-700,00		
+ 5505 Infopelare Klemetsby	-136,00	-680,00			
[-] C550 Parker och allmänna områden	-16 024,09	-18 321,00	-3 098,00		
+ 5502 Badstrand Kapellviken	-3 152,92	-2 650,00	-650,00		
+ 5506 Allmänna områden, ofördelat	-5 052,00	-3 099,00	-1 000,00		
+ 5507 Lekpark Hågen	-1 257,00	-2 489,00			
+ 5509 Fotbollsplan Klemetsby	-3 403,04	-5 742,00	-500,00		
+ 5510 Motionsbana Furuborg	-1 975,23	-2 611,00	-348,00		
+ 5951 Mattvätt	-1 183,90	-1 730,00	-600,00		
[-] C555 Hamnverksamhet	-577,00	-1 688,00			
+ 5551 Kapellhagens båthamn	-577,00	-1 688,00			
[-] C560 Byggnader o. lokaler / offentliga	-177 751,10	-170 240,00	-101 280,00		
+ 5601 Kommunkansliet	-11 557,60	-16 184,00	-8 190,00		
+ 5602 Grundskolan	-67 943,64	-52 130,00	-33 420,00		
+ 5604 Slöjdsalen	-1 827,67	-2 696,00	-2 900,00		
+ 5605 Lidret	-488,94	-2 010,00	-200,00		
+ 5606 Branddepån	-16 105,97	-20 349,00	-12 050,00		
+ 5607 Daghemmet Videungen	-20 563,93	-18 104,00	-8 020,00		
+ 5608 Daghemmet Myrstacken	-6 560,18	-7 514,00	-6 660,00		
+ 5655 Prästgårdsvägen 1-3	-52 703,17	-51 253,00	-29 840,00		
[-] C565 Byggnader o. lokaler / hyresbostäder	37 224,85	37 552,00	108 952,00		
+ 5653 Prästgårdsvägen 5 och 7	15 384,98	20 950,00	31 413,00		
+ 5654 Kapellvägen 2	25 143,87	16 602,00	27 089,00		
+ 5656 Fjärilsgränd	-3 304,00		50 450,00		
[-] C570 Intern service	-4 509,87	-104,00	-73 516,00		
+ 5701 Fastighetservice och uthyrningstjänster	-224,71	-104,00	-69 316,00		
+ 5609 Lager	-4 285,16		-4 200,00		
[-] C580 Vattenverk	12 041,33	6 999,00	24 186,00		
+ 5801 Vattendistribution	12 041,33	6 999,00	24 186,00		
[-] C585 Avloppsverk	-30 868,92	-10 280,00	23 028,00		
+ 5851 Rensningsverk Långnäs	-40 868,92	-20 280,00	29 028,00		
+ 5852 Avloppsledningar	10 000,00	10 000,00	-6 000,00		
Totalsumma	-235 286,79	-212 603,00	-87 128,00	-87 999,28	-88 879,27

Anslagsansvarig

Tekniska chefen.

Tekniska sektorn sköter administrationen och utförandet kopplat till bland annat fastighetsunderhåll, trafikleder samt vatten- och avloppsverksamhet. Visionen för verksamheten är att förvalta kommunens egendom så att den bibehåller sitt värde samt fyller sin funktion, att minska miljöbelastningen genom åtgärder inom bland annat enheternas avfallshantering, avloppsvattenbehandlingen samt energisparande åtgärder, att minimera personalomsättningen och motivera de anställda till goda arbetsresultat.

Den av tekniska sektorn förvaltade egendomen används bland annat för att bedriva den offentliga kommunala servicen såsom äldreomsorg, barnomsorg samt skola, för invånar-



nas rekreation och välbefinnande samt för att tillse ren-, och avloppsvattenleveranser för anslutna kunder.

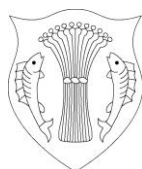
7.8.1.1. Verksamhets- och volymförändringar under budgetåret

Sett till inflationen verkar läget nu som att det har stabiliserats en aning. Och förhoppningsvis håller sig inflationen på en sådan nivå att höjningen av taxorna ska ge den beräknade kostnadstäckningen.

Nytt för året är att Lumparland har en helt fristående budget. Den är alltså inte längre en del av Lemlands budget.

7.8.1.2. Verksamhetsmål 2025

Mål:	Metod:
1. Förtydliga förväntningar och förutsättningar för alla tjänster och befattningar inom sektorn. Effektivisera beslutsgångar.	1. Uppdatera tjänste-, och befattningsbeskrivningar. Uppgöra en plan och prioritering på övergripande processer. Påbörja framtagande av övergripande processer för att skapa en tydlig helhetsbild utgående från planen.
2. Underhållsplanering	2. Att kartlägga tekniska sektorns ansvarsområden. Skapa underhållsplaner för allting som ligger inom ansvarsområdet.
3. Processbeskrivning återkommande arbetsuppgifter	3. Framtagande av processbeskrivningar för att effektivisera det dagliga arbetet och skapa ett bättre flöde i verksamheten.
4. OVK i kommunens byggnader.	4. Följa OVK-planen.



7.8.1.3. Verksamhetsmål 2026–2027

Mål:	Metod:
1. Effektivisera beslutsgångar	1. Fortsatt arbeta med medframtagande av övergripande processer. Utgående från upphandlingar av ramavtal delegera avrop till personal inom sektorn.
2. Systemstöd	2. I samråd med övriga sektorer fortsätta arbetet med utvecklingen av sektorns systemstöd.
3. Inmätning av VA-infrastruktur	3. Sluför inmätningen av befintlig VA-infrastruktur.

7.8.2. Tekniska kansliet

Resultatenheten omfattar tekniska kansliet. Tekniska kansliet sköter administrationen kopplat till bland annat fastighetsunderhåll, trafikleder samt vatten- och avloppsverksamhet. Visionen för verksamheten är att förvalta kommunens egendom så att den bibehåller sitt värde samt fyller sin funktion, att minska miljöbelastningen genom åtgärder inom bland annat avfallshantering samt avloppsvattenbehandlingen, att minimera personalomsättningen och motivera de anställda till goda arbetsresultat. Tekniska kansliet är från 1.1.2025 en köptjänst från Lemlands kommun.

7.8.3. Trafikleder

Resultatenheten omfattar väghållning av kommunalvägar samt sommar- och vinterunderhåll av byggnadsplanevägar och gång- och cykelvägar. Underhållet handhas i huvudsak av privata entreprenörer. I verksamheten ingår även att upprätthålla vägbelysningen i kommunen. Visionen för verksamheten är trafiksäkra vägar som så bra som möjligt tillgodoser användarnas behov.

NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Lumparland			
Kommunalvägar (km)	2,55	2,55	2,55
Byggnadsplanevägar (m)	1 530	1 530	1 530
Gång- och cykelvägar (m)	4 850	4 850	4 850
Rastplatser (st)	1	1	1
Vägbelysning, armaturer (st)	55	55	55
Privatvägsplogning (st)	32	28	28

7.8.4. Parker och allmänna områden

Resultatenheten omfattar underhåll av idrotts- och friluftsanläggningar i kommunen. Dessa är i Lumparland, gräsplanen i Klemetsby, badstränderna samt övriga friluftsområden och lekplatsen vid Kapellviken. Underhållet handhas i huvudsak av kommunens en-



het för fastighetsskötsel. Visionen för verksamheten är att till kommunmedlemmar, sommargäster och turister erbjuda ändamålsenliga och välskötta anläggningar och områden för ledd och fri fritidssysselsättning.

NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Anläggningar i Lumparland (exklusive diverse allmänna områden)			
Idrottsplaner (st)	1	1	1
Konditionsbanor (st)	1	1	1
Badstränder (st)	1	1	1
Mattvätt (st)	1	1	1
Lekparker (st)	1	1	2
Totalt (st):	5	5	6

7.8.5. Hamnverksamhet

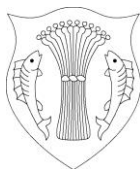
Resultatenheten omfattar underhåll och uthyrning av platser i Kapellviken (fyra platser). Visionen för verksamheten är en hög uthyrningsgrad samt nöjda båtägare.

NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Uthyrda småbåtsplatser:			
Kapellviken	0	0	4
Totalt (st):	0	0	4
Sjösättningsramper (st)	0	0	0

7.8.6. Byggnader och lokaler

Resultatenheten omfattar Lumparlands verksamhetslokaler för olika typer av främst offentlig verksamhet. I byggnaderna verkar i huvudsak kommunernas egna verksamhetsenheter. Visionen för verksamheten är att erbjuda trivsamma och ändamålsenliga arbets- och verksamhetsutrymmen för kommunens olika verksamhetsenheter samt en fastighetsförvaltning som fungerar ändamålsenligt och ekonomiskt.

Lumparlands kommuns byggnader är grundskolan jämte biblioteket, kommungården, branddepån, Kapellhagen samt daghemmen Videungen och Myrstacken.



NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Lumparland			
Skola & bibliotek (st)	1	1	1
Daghem (st)	1	1	1
Servicehus för äldre (st)	1	1	1
Kommunkansli (st)	1	1	1
Branddepå (st)	1	1	1
Totalt (st):	5	5	5
Förbrukning av eldningsolja (m ³) Lemland	6	5	2
Förbrukning av eldningsolja (m ³) Lumparland	0	0	0

7.8.7. Hyresbostäder

Resultatenheten omfattar i huvudsak uthyrning av bostadslägenheter. Lumparlands kommuns hyresbyggnader är Prästgårdsvägen 5 och 7, Kapellvägen 2 och Fjärilsgränd 2. Totalt 18 lägenheter. Visionen för verksamheten är att erbjuda trivsamma och ändamålsenliga bostadslägenheter för Lumparlands kommuns hyresgäster samt en fastighetsförvaltning som fungerar ändamålsenligt och ekonomiskt.

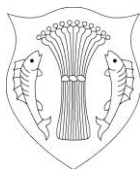
NYCKELTAL	Bokslut 2023	Budget 2024	Budget 2025
Bostadsradhus (st)	3	3	3
Parhus (st)	0	0	3
Hyreslägenheter (st)	12	12	18
Uthyrningsgrad (%)	100,0%	100,0 %	100,0 %

7.8.8. Fastighetsunderhåll

Resultatenheten omfattar i huvudsak enheten för fastighetsskötsel samt där tillhörande anslag för personalkostnader och för fordon och övrig gemensam utrustning. Uppgiftsområdets kostnader fördelas internt på servicens användare. Fastighetsskötseln upprätthåller beredskap dygnet runt. Genom att tillämpa systematiska arbetssätt vid rätt tidpunkt och i rätt omfattning är visionen för verksamheten att utföra underhållsåtgärder som på sikt minimerar behovet av reparationer och minskar risken för att akuta situationer uppstår.

7.8.9. Vatten- och avloppsverk i Lumparland

Resultatenheten omfattar distribution av dricksvatten samt emottagande och transport av avloppsvatten. Dricksvattnet köps av Ålands Vatten Ab. Avloppsvattnet transporteras med hjälp av pumpstationer till kommunens eget reningsverk i Långnäs där det renas. Visionen för verksamheten är att distribuera dricksvatten av hög och jämn kvalitet till alla abonnenter inom vattenverkets verksamhetsområde, att kunna ta emot avloppsvatten samt effektivt och ekonomiskt transportera det till reningsverket i Långnäs där det



Budget 2025 och ekonomiplan 2026–27 för Lumparlands kommun

renas med bästa möjliga teknik så att miljöbelastningen blir så liten som möjligt samt att maximera vatten- och avloppsanslutningarna inom verksamhetsområdet.

NYCKELTAL	Budget 2023	Budget 2024	Budget 2025
Vattenledningsnät, Lumparland			
Abonnenter (st)	241	222	230
Tryckförhöjningsstationer (st)	0	0	0
Köpt renvatten (m ³)	25 000	25 000	25 250
Sålt renvatten (m ³)	18 500	18 500	18 750
Täckningsgrad, extern (%)	137,1 %	121,1 %	121,1 %
Täckningsgrad, totalt exkl. avskrivningar (%)	117,3 %	95,9 %	95,9 %
Avloppsledningsnät, Lumparland			
Abonnenter (st)	56	56	62
Pumpstationer (st)	6	6	6
Inkommet avloppsvatten (m ³)	7 000	7 050	7 050
Fakturerat avloppsvatten (m ³)	4 600	4 850	5 370
Slam externt (m ³)	1 000	1 000	0



7.9. Brand- och räddningsväsendet (Ålands räddningsmyndighet)

C 6 0 0 Brand och räddning	Bokslut 2023	Budget 2024	Budget 2025	EP 2026	EP 2027
▢ C 6 1 0 Brandskydd	-35 712,25	-36 770,00	-28 975,00		
▣ 6 1 0 1 Räddningsnämnden	-35 712,25	-36 770,00	-28 975,00		
▢ C 6 2 0 Befolkningsskydd	-4 393,86	-6 139,00	-4 090,00		
▣ 6 2 0 1 Befolkningsskyddet	-4 393,86	-6 139,00	-4 090,00		
To tals umma	-40 106,11	-42 909,00	-33 065,00	-33 395,65	-33 729,61

Anslagsansvarig

Räddningschefen.

Räddningsmyndigheten handhar förutom det förebyggande tillsynsarbetet även räddningsledarfunktionen och därtill en koordinerande roll gällande beredskapsärenden och befolkningsskyddet. Information till allmänheten och till de kommunala enheterna ska skötas centralt från räddningsmyndigheten.

Jomala kommun är huvudman för räddningsmyndigheten.

7.9.1. *Räddningsnämnden*

Kostnadsstället avser kostnader för den gemensamma räddningsnämnden för Ålands Räddningsmyndighet där kommunen har en representant. Kostnaderna för verksamheten fördelas enligt invånarantal.

I kostnadsstället ingår också ersättning till Lumparlands FBK som avtalsbrandkår.

Målsättningar 2025

- Under året få myndigheten på plats.
- Framta styrdokument till kommunernas servicenivå.
- Framta styrdokument för samarbetet mot kommunernas byggnadsinspektioner.
- Framta styrdokument till kommunerna för en revidering av avtal mot avtalsbrandkår.

7.9.2. *Befolkningsskyddet*

Kostnadsstället avser kostnader för räddningsmyndighetens koordinerande roll gällande beredskapsärenden och befolkningsskyddet.

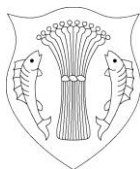


8. INVESTERINGARNA

Kostnadsställe 8301					
Projektets namn Hyresbostäder					
	Beräknad anv. per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	Totalt för investeringen
Kostnader	-	- 15 000,00	-	-	- 15 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	- 15 000,00	-	-	- 15 000,00
Beskrivning av investeringen Målning av fasader på hyreslägenheter, Kapellvägen 2, Prästgårdsvägen 5-7.					

Kostnadsställe 8304					
Projektets namn Parhuslägenheter					
	Beräknad anv. per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	Totalt för investeringen
Kostnader	-	- 40 000,00	-	-	- 40 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	- 40 000,00	-	-	- 40 000,00
Beskrivning av investeringen Markbereda och asfaltera väg, parkering och gångstråk vid Fjärilsgränd 2.					

Kostnadsställe 8558					
Projektets namn Inventarier FBK					
	Beräknad anv. per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	Totalt för investeringen
Kostnader	-	- 10 000,00	- 15 000,00	-	- 25 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	- 10 000,00	- 15 000,00	-	- 25 000,00
Beskrivning av investeringen Förnyande av andningspaket samt radio inom rökskyddet under år 2025 då nuvarande är föråldrade. Inköp av klippustrustning planeras under 2026.					



Budget 2025 och ekonomiplan 2026–27 för Lumparlands kommun

Kostnadsställe 8563 Projektets namn Båtbyte FBK					
	Beräknad anv.				Totalt för
	per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	investeringen
Kostnader	-	-	- 35 000,00	-	- 35 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	-	- 35 000,00	-	- 35 000,00
Beskrivning av investeringen Ett båtbyte planeras till år 2026 för Lumparlands frivilliga brandkår.					

Kostnadsställe 8801 Projektets namn Vattenledningar					
	Beräknad anv.				Totalt för
	per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	investeringen
Kostnader	-	- 10 000,00	- 10 000,00	- 10 000,00	- 30 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	- 10 000,00	- 10 000,00	- 10 000,00	- 30 000,00
Beskrivning av investeringen Ospecificerade vattenledningar.					

Kostnadsställe 8805 Projektets namn Ospecificerade avloppsledningar					
	Beräknad anv.				Totalt för
	per 31.12.2024	Budget 2025	Plan 2026	Plan 2027	investeringen
Kostnader	-	- 10 000,00	- 10 000,00	- 10 000,00	- 30 000,00
Intäkter	-	-	-	-	-
Landskapsandelar	-	-	-	-	-
Nettokostnad	-	- 10 000,00	- 10 000,00	- 10 000,00	- 30 000,00
Beskrivning av investeringen Ospecificerade avloppsledningar					

Anledningar till ramöverskridningar

I budgetdirektivet för budget 2025 ska förvaltningarna inkomma med en motivering varför eventuell ramöverskridning sker. Barnomsorgen, grundskolan och äldreomsorgsförvaltningen har överskridit kommunstyrelsens fastslagna ramar. För se anledningarna till ramöverskridningarna har budgetförslag för 2025 jämförts med bokslut 2023. Samtidigt jämförs dessa skillnader mot den fastslagna ramen.

Barnomsorg

Barnomsorgen går enligt liggande förslag över ramen med 45 095,62 euro. I Bokslut 2023 har en inkomst för barn från annan kommun bokförts på cirka 81 000 euro. I budgetförslaget för 2025 är den summan budgeterad till 50 000 euro. I övrigt är det ökningen av en barnskötare från 75 procent till 100 procent som gör den övriga skillnaden. Ökningen av barnskötaren till 100 procent ses som helt nödvändig för att daghemsföreståndaren ska kunna hinna med all administration, vilken uppskattas ta två dagar i veckan i anspråk. Många kommuner har redan övergått till helt administrativa daghemsföreståndare, och att bibehålla endast en administrationsdag är inte möjlig med nuvarande krav på dokumentation, arbete med läroplaner och övriga styrdokument som ska tas fram tillsammans med landskapet, exempelvis IKT-strategi för barnomsorgen.

Lumparlands skola

Lumparlands skola går över ram med 47 579,10 euro. Den inkomst som tidigare var på daghemmet är nu på Lumparlands skola vilket medför ökade inkomster med cirka 50 000 euro mot bokslut 2023. Detta äts dock upp av att budgetförslaget för 2025 bygger på tre klasser istället för tidigare två klasser. I budgetförslaget finns alltså en ytterligare timlärare från hösten 2025. Därutöver finns en assistent budgeterad från och med hösten 2025. Skolskjutskostnaderna ökar något mot bokslut med detta beror på att elev på Ängö-Bussö har skolskjuts. Denna summa faktureras vidare till Vårdö och är således ett nollsummespel för kommunen.

Det är värt att nämna att budgetförslaget för 2025 är lägre än det slutliga resultatet för år 2023 med cirka 6 000 euro. Det beror förstås till stor del att skolan arbetar läsårsvis medan budgeten är årsvis. Om tre klasser var budgeterat för hela år 2025 skulle budgeten också överskrida bokslut 2023-

Kyrkby högstadieskola inkl. SÅUD:s förvaltning

Trots att elevantalet går ner överskrider SÅUD sin ram för kommunen med 26 319 euro. Detta beror på att utbyggnationen av KHS fördelas ut enligt avskrivning per elev. Därutöver ökar talterapitjänsterna samt genomförs kollektivavtalsenliga löneförhöjningar.

Äldreomsorgsförvaltningen

Äldreomsorgsförvaltningen överskrider ramen med 193 080,78 euro. Vid en jämförelse med bokslut 2023 kan konstateras att Kapellhagen inte längre har någon klient från annan kommun vilket minskar inkomsterna med cirka 65 000 euro. Den nya klientavgiftslagen medför att kommunen inte längre får ta någon separat måltidsavgift. Detta minskar inkomsterna ytterligare med cirka 37 000 euro. Dessa kompenseras i viss mån av ökade inkomster på serviceboendeavgifterna genom att dessa ökar med cirka 16 000 euro. Nettot är dock negativt för kommunen.

Införandet av Cosmics externa journal tillsammans med ÅHS ökar ICT-kostnaderna med cirka 8 000 euro.

Korrigerings av Sveagårdens dygnsavgift ökar kostnaderna med cirka 45 000 euro.

Närståendevården budgeteras högre med cirka 18 000 euro.

Avslutningsvis tillkommer kollektivavtalsenliga löneförhöjningar, men ingen ökning i personalstyrkan är budgeterad. I bokslut 2023 fanns ingen anställd kock, vilket gör att lönekostnaderna blir väsentligt högre i budget 2025.

Sammanlagt har kommunens nettokostnader från bokslut 2023 till budget 2025 ökat med cirka 230 000 euro, vilka kan hänföras till 86 000 euro i minskade inkomster för klient från annan kommun samt serviceavgifter, 45 000 euro i ökade kostnader för klient placerad i annan kommun och 18 000 i ökade utgifter för närståendevård, totalt 149 000 euro. Övrigt är löneförhöjningar, anställd kock på 80 procent och inköp av ICT-system.

Konsekvenser av nedskärningar

Barnomsorg

Ifall kommunstyrelsen skulle bibehålla barnskötaren på 75 procent för 2025 skulle daghemmet inte hinna med den administrationen utan att daghemsföreståndaren skulle behöva jobba övertid. Daghemsföreståndaren har nämligen redan under 2024 jobbat mer än ordinarie arbetstid för att hinna med. Förvaltningen ser därför inte att det är möjligt att under 2025 ha barnskötaren på under 100 procent.

Lumparlands skola

Ifall kommunstyrelsen beslutar ta bort den ytterligare läraren samt assistenten behöver skolan fortsätta att ha endast två klasser, 1-3 och 4-6. 1-3 skulle bli tretton elever (8+2+3) och 4-6 skulle bli åtta elever (1+1+6). Det är värt att nämna att den ytterligare assistenten är med i budgeten på grund av att det elever med särskilda behov väntas öka från höstterminen 2025, så att ta bort assistenten kan försvåra för dessa elevers skolgång.

Äldreomsorgsförvaltningen

För att öka inkomsterna skulle kommunen kunna erbjuda en lägenhet till andra kommunen. Det är under förutsättning att kommunen inte behöver den för sina egna klienter. Som det ser ut nu skulle det vara riskabelt att hyra ut en lägenhet till en annan kommun.

Att ta hem klienter som bor på annat serviceboende med heldygnsomsorg ser ut att bli väsentligt dyrare än att ha dem placerad i annan kommun, på grund av att kommunen skulle behöva anställa väsentligt mer personal. Detta bereds dock inom ramen för ett annat ärende.

Att sänka närståendevårdens anslag riskerar att fler anlitar kommunens hemservice istället för att utföra närståendevård. Närståendevård är för kommunens kostnader det mest förmånliga alternativet och bör premieras.

Vad gäller klientavgifterna har kommunen redan de högsta som lagen tillåter. Dessa avgifter förväntas dock öka med tiden då pensionerna ser ut att öka eftersom avgifterna är inkomstbaserade.

Väsentliga skillnader bokslut 2023 mot budget 2025	Bokslut 2023	Budget 2025	Skillnad
2211 Daghemmet Videungen och Myrstacken			
3116 Elev från annan kommun	81 307,90	50 000,00	-31 307,90
4000 Ordinarie löner	-159 256,56	-169 855,00	-10 598,44
4025 Tidsbunden	-14 857,20	-40 822,00	-25 964,80
A4130 Lönebikostnader Summa	-40 198,53	-53 438,70	-13 240,17
Totalt	-133 004,39	-214 115,70	-81 111,31
Ram	-230 000,00		
Budgetförslag 2025	-275 095,62		
Ramöverskridning	-45 095,62		

Väsentliga skillnader bokslut 2023 mot budget 2025	Bokslut 2023	Budget 2025	Skillnad
3201 Lågstadiet			
3116 Elev från annan kommun	41 175,92	90 849,00	49 673,08
	A4120 Löner och arvoden Summa	-219 522,54	-53 309,46
	A4130 Lönebikostnader Summa	-60 187,70	-14 152,57
4310 Köp av kommuner		-6 000,00	-6 000,00
4311 Köp av kommunalförbund	-3 503,11	-7 110,00	-3 606,89
4420 Rese- och transporttjänster	-41 656,46	-55 000,00	-13 343,54
3205 Lågstadieelever i andra kommuner			
4310 Köp av kommuner	-45 498,06		45 498,06
Totalt	-315 039,38	-310 280,70	4 758,68
Ram	-325 000,00		
Budgetförslag 2025	-372 579,10		
Ramöverskridning	-47 579,10		

Tillsyn av hemundervisade barn, eventuellt för högt budgeterat
 Talterapijänster har tillkommit

Väsentliga skillnader bokslut 2023 mot budget 2025

	Bokslut 2023	Budget 2025	Skillnad
3202 Högstadiet			
4311 Köp av kommunalförbund	-283 523,06	-243 319,00	40 204,06
3203 Träningsundervisningen			0,00
4311 Köp av kommunalförbund	-46 853,31		46 853,31
Totalt	-330 376,37	-243 319,00	87 057,37
Ram	-217 000,00		
Budgetförslag 2025	-243 319,00		
Ramöverskridning	-26 319,00		

Väsentliga skillnader bokslut 2023 mot budget 2025	Bokslut 2023	Budget 2025	Skillnad
2331 Hemvård			
A4120 Löner och arvoden Summa	-47 719,16	-55 510,00	-7 790,84
A4130 Lönebikostnader Summa	-10 565,60	-13 131,30	-2 565,70
4361 Data och telekommunikationstjänster (ICT)	-641,00	-2 313,00	-1 672,00
4840 Hyror för maskiner och inventarier	-719,64	-8 500,00	-7 780,36
2334 Kapellhagens serviceboende			0,00
A3150 Ersättningar av kommuner och samkommuner Summa	65 033,14		-65 033,14
A3200 Socialväsendets avgifter Summa	43 382,12	60 000,00	16 617,88
A3230 Övriga serviceavgifter Summa	37 563,67		-37 563,67
A4120 Löner och arvoden Summa	-457 010,92	-499 570,00	-42 559,08
A4130 Lönebikostnader Summa	-101 167,84	-118 179,80	-17 011,96
4361 Data och telekommunikationstjänster (ICT)	-14 852,11	-23 000,00	-8 147,89
4840 Hyror för maskiner och inventarier	-8 427,94	-1 000,00	7 427,94
2336 Serviceboende i annan kommun			0,00
4310 Köp av kommuner	-130 670,00	-176 300,00	-45 630,00
2423 Närståendevärd			0,00
2423 Närståendevärd Summa	-8 903,06	-27 076,50	-18 173,44
Totalt	-634 698,34	-864 580,60	-229 882,26
Ram	-750 000,00		
Budgetförslag 2025	-943 080,78		
Ramöverskridning	-193 080,78		

Leasingbilen flytta till hemvård, nollsummespel

Leasingbilen flytta till hemvård, nollsummespel

Ökningen beror på värdinformationssystem, eventuellt för högt budgeterad.

Leasingbilen flytta till hemvård, nollsummespel

Nyckeltal	Rapport	Typ av nyckeltal	Årsad	Kumulera	Lumoartad	Värde	Sund	Flekt	Bränd	Geta	
Äldre (boende) ESB	budget 2024	Äldreomsorg		11	11		13	10	15	10	9
Antal vårdögn externa socialrådgivare (Olson, Steffensen hemmet, specialjukavdel)	budget 2024	Äldreomsorg									
				605	0		365	730	0	160	366
Kostnad äldreomsorg/vård dag	bokslut 2023	Äldreomsorg					164,86	217,21	205 (ESB)		217,68
				168,87	184,98						
Kostnad äldreomsorg/mfE utöver brutto ESB inkl. hemservice	bokslut 2023	Äldreomsorg									
				3412,25	2 699		2048,8	2 165	2486,5	2465,59	1913,55
Kostnad äldreomsorg/klent utöver brutto ESB o Hemservice	bokslut 2023	Äldreomsorg									
				68429,79	72 188		61597	110623,21	74823 (ESB)		69521
Kassa 31.12	bokslut 2023	Balansräkning		518707	161669		715000	1998665	1888000	2431233	600113
Förändring likvida medel	bokslut 2023	Balansräkning		-28687	-352935		309000	-173000	-309000	228000	66583
Befolkning 31.12	bokslut 2023	Befolkning	####	290	366		471	995	509	436	509
Befolkning 31.12	budget 2024	Befolkning		297	366			995	504	436	503
Barn 0-6 år	budget 2024	Daghem									
				13	20		79	95	28 (på daghem)	12 på daghem (15:1 kommunera)	30
Kostnad allmän förvaltning	budget 2024	Kostnader									
				197 680	210508		278034	387260	303000	356953	326800
Kostnad per portion (brutto)											
Antal portioner											
Bruttokostnad centralkök	budget 2024	Kostnader									
				23762	Har ej centralkök		Har ej	Har ej	23600		32272
Kostnadsäckning byggskriv	bokslut 2023	Kostnader		36,71 %	46,00 %		17,90 %	60,90 %			c. 50%
Kostnadsäckning pufall	bokslut 2023	Kostnader		90,73 %	Misc		100 %	103,80 %	101,90 %	82,5 %	86 %
Kostnadsäckning avlopp	bokslut 2023	Kostnader		48,17 %	100 %		44 %	60,50 %	105 %		87 %
Kostnadsäckning vatten	bokslut 2023	Kostnader		25,70 %	100 %		90 %	80,50 %	87,80 %	Enskilda vattenlåg	87 %
Kostnadsäckning snölogpning	bokslut 2023	Kostnader		39,62 %	139,23 %		MINUS	100 %	ca 85 % för privata våcar	erbjuddt ei	



Avgifter för annonsering i infobladet och kopiering

Dnr: 264/2024

Antagna av kommunfullmäktige genom § xx/xx.11.2024 att gälla från och med 1.1.2025.

Samtliga avgifter är inklusive moms 25,5 %.

Infobladet

<i>Annonsering</i>	<i>Euro</i>
1/1 sida	30,00
1/2 sida	20,00
1/4 sida	15,00
<i>Prenumeration</i>	<i>Euro</i>
Infobladet/år	50,00

Privatpersoner bosatta i Lumparland får avgiftsfritt införa en annons på 1/4 sida per infoblad.

Föreningar i Lumparland får avgiftsfritt införa en annons på 1/1 sida per infoblad.

Kommunalförbund i vilka Lumparlands kommun är medlem och kommuner med vilka Lumparlands kommun har samarbetsavtal får avgiftsfritt införa annonser i infobladet.

Kommunen förbehåller sig rätten att besluta om en annons eller skrivelse publiceras.

Kopior och utskrifter

De 10 första svartvita kopiorna är avgiftsfria. Färgkopior kostar från första kopian.

Ensidiga kopior

<i>Svartvita</i>	<i>Euro</i>	<i>Färg</i>	<i>Euro</i>
A4	0,90	A4	1,00
A3	1,00	A3	1,10

Dubbelsidiga kopior

<i>Svartvita</i>	<i>Euro</i>	<i>Färg</i>	<i>Euro</i>
A4	1,10	A4	1,20
A3	1,35	A3	1,45



Allmännyttiga samfund i Lumparland kopierar svartvita kopior avgiftsfritt.

Utlämnande av uppgift som kräver särskilda åtgärder

Vid begäran om uppgifter som kräver omfattande informationssökning tas en avgift ut som motsvarar kostnaderna för att ta fram uppgifterna, om det inte är fråga om skyldigheten att ge råd, höra eller informera.

För utlämnande av en uppgift ur en handling, kopia eller någon annan utskrift som kräver särskilda åtgärder tas en fast grundavgift ut som varierar beroende på hur krävande informationssökningen är:

Normal informationssökning (arbetstid under 2 tim)	40,00 euro
Krävande informationssökning (arbetstid 2–5 tim)	100,00 euro
Mycket krävande informationssökning (arbetstid över 5 tim.)	160,00 euro

Kräver informationssökningen mer än en dag är avgiften 160 euro/dag.

Utöver grundavgiften tas kopieringsavgift för varje sida enligt priset för kopior och utskrifter.

En fast avgift som graderats på ovan nämnda sätt tillämpas också när särskilda åtgärder krävs vid informationssökningen för utlämnandet av en uppgift ur en handling muntligen, när handlingen ges för läsning eller när uppgiften sänds per e-post.

Avgiftsfria handlingar

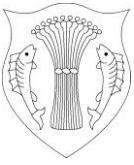
Avgift tas inte då beslut genom protokollsutdrag delges part. Avgift betalas inte heller för handling enligt vilket det enligt lag eller förordning inte ska betalas.

Information ur handlingar avgiftsfri när:

- uppgifterna ges muntligt
- handlingen läses eller kopieras hos myndigheten
- en handling som lagrats elektronisk sänds per e-post
- när utlämnandet av handlingen ingår i myndighetens skyldighet att ge råd, höra eller informera.

Avgift betalas inte heller:

- av den egna kommunens eller kommunalförbunds myndigheter och inrättningar
 - för arbetsintyg, löneintyg, matrikelutdrag eller en handling som behövs för ansökan om pensions- eller annan förmån och som grundar sig på ett pågående eller avslutat tjänste- eller arbetsförhållande till kommunen
 - av den egna kommunens eller den egna samkommunens förtroendevalda för handlingar som han eller hon finner behövliga för sitt uppdrag
-



Lumparlands kommun

- för en handling som enligt lag ska utges till en statlig myndighet
 - för kopiering av handling som lämnas in till kommunal myndighet.
-



Avgifter för tillstånd för försäljning av nikotinpreparat samt inspektion

Dnr: 265/2024

Antagna av kommunfullmäktige genom § xx/xx.11.2024 att gälla från och med 1.1.2025.

Försäljning av nikotinpreparat på andra ställen än apotek förutsätter ett detaljhandelstillstånd för nikotinpreparat. Tillståndet ansöks vid den kommun som försäljningsplatsen ligger i.

Detaljhandelstillstånd för nikotinpreparat avsedda för att dra ner på och sluta röka kan beviljas affärer, servicestationer, kiosker och näringsställen. Att sälja nikotinpreparat i automater är förbjudet.

Av ansökan ska framgå:

1. sökandens namn eller sammanslutningens firma och kontaktuppgifter, företags- och organisationsnummer samt adresserna till de försäljningsställen där nikotinpreparat säljs
2. hur nikotinpreparaten förvaras samt arrangemangen för övervakning av försäljningen
3. den försäljningsansvariges namn och kontaktuppgifter
4. antalet säljställen och hur de är placerade på försäljningsstället.

Lumparlands kommun underrättar Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea när tillstånd har beviljats.

Avgifter

1 § Tillstånd för försäljning av nikotinpreparat
105 euro.

2 § Inspektion
68 euro per påbörjad timme.

Bygglovstaxa 2025

Bilaga A – Ks § 154

AVGIFTER FÖR TILLSYN ÖVER BYGGNADSARBETE, AVLOPPSANLÄGGNINGAR OCH FÖR INSPEKTION AV SAMLINGSLOKALER SAMT FÖR HÖRANDE AV GRANNE MM I LUMPARLANDS KOMMUN

1 §

Allmänt

Byggherre eller den som vidtar åtgärd är skyldig att till kommunen erlægga avgifter som bestäms i denna taxa för sådana inspektions- och tillsynsuppgifter som är nödvändiga för att fullfölja byggnadsarbetet (99 § plan- och bygglagen, PBL).

För inspektion av samlingslokaler är sökande skyldig att erlægga avgifter som bestäms i 6 § i denna taxa med stöd av 19 och 20 §§ LL om offentliga nöjeställningar.

Avgifterna över byggnadsarbete och inspektion av samlingslokaler inkluderar lösen av handlingarna.

Byggnadslovsavgifterna är inte momspliktiga.

2 §

Uppförande av nybyggnad och därmed jämförbara ändringar (66 § i PBL)

	<u>Taxa €</u>
2.1 Uppförande av nybyggnad, per byggnad därtill enligt byggnadens våningsyta (per m ²)	376,44 2,28
2.2 Uthyrningsstuga	
Då byggnadslovet omfattar flera stugor som byggs enligt samma ritning i grupp, erläggs full avgift för en stuga. För därpå följande stugor erläggs 50 % av avgiften, per byggnad	376,44
Därtill enligt byggnadens sammanlagda våningsyta (per m ²)	2,28
2.3 Tillbyggnad, ombyggnad, per byggnad därtill enligt tillbyggnadens våningsyta (per m ²)	199,31 2,28
2.4 Ekonomibyggnad och dylikt, per byggnad därtill enligt byggnadens våningsyta (per m ²)	199,31 0,87
2.5 Ändring av användning, per byggnad därtill enligt byggnadens våningsyta (per m ²)	199,31 2,28
2.6 Fasadändring, takändring (inklusive skärmtak >12 m ²), ändring av bärande konstruktioner	78,95
2.7 Installation eller ändring av eldstad, rökkanal eller hiss	78,95
2.8 Tillfälliga byggnader, samma som varaktig	

Taxa €

2.9	Uppförande av sol- och vindkraftverk/st	
-	som betjänar flera än 3 hushåll, effekt max 0,5 MW	199,31
-	Effekt 0,5 - 3 MW	397,86
-	Effekt över 3 MW	752,79

3 §

Avgifter för övriga tillståndsbeslut i byggnadsärenden (67 § i PBL) 78,95

3.1	Nöjespark, idrotts- eller campingplats	
3.2	Skjut- eller motorbana	
3.3 a	Småbåtshamn med flera än 10 båtplatser	
3.3 b	Kajer, broar, vågbrytare, kanaler och dylikt.	
3.4	Cistern eller dylikt > 10 m ³	
3.5	Mast högre än 25 meter	
3.6	Torn tillgängligt för allmänheten	
3.7	Tillståndspliktigt plank eller mur	
3.8	Husvagn, buss eller dylikt (utanför campingplats) som skall användas för boende, affärslokal eller dylikt > 2 månader	

4 §

Avgifter för övriga beslut i byggnadsärenden 78,95

4.1	Utbyte av ritning	
4.2	Förhandsutlåtande	
4.3	Förlängning av byggnadslovens giltighetstid (75 § i PBL)	
4.4	Tillstånd att börja byggnadsarbete (innan beslutet vunnit laga kraft) (76 § i PBL)	
4.5	Bod samt fristående carport om max 25 m ²	
4.6	Behandling av rivningsanmälan (69 § i PBL)	

5 §

Förhöjd avgift vid byggande utan bygglov

Om byggherren har påbörjat byggnadsarbetet innan bygglovet har beviljats, eller anmälan inlämnats, utgår en förhöjd avgift om 50 %. Detta gäller samtliga avgifter kopplade till bygglovet. Den förhöjda bygglovsavgiften är inte ett straff utan en ersättning för det merarbete det innebär för byggnadstillsynen att bereda och behandla ett ärende om byggande utan bygglov.

6 §

Godtagbar säkerhet i enlighet med PBL 76 §

En godtagbar säkerhet kan vara en bankgaranti eller en deposition på kommunens konto.

Den godtagbara säkerhetens storlek utgörs av;

grundsumma per byggnad	1175,25
därtill enligt byggnadens bottenyta upp till 500 m ² (per m ²)	41,22
för bottenyta över 500 m ² utgår (per m ²)	17,49

Säkerheten återbördas till byggherren då bygglovet vunnit laga kraft.

7 §**Syner**

Vid utförande av de i § 3 nämnda byggnadsåtgärderna skall avgift erläggas för förrättande av de syner som kan komma ifråga enligt följande:

7.1	Syn som förrättas under byggnadstiden	35,17
7.2	Slutsyn	48,27
7.3	Avgifter som rör brandsyneverksamheten, men som debiteras i samband med byggnadslovsavgifterna	
	- Kanal- och eldstadssyn	56,00
	- Ventilationssyn	56,00
	- Ibruktagningssyn	56,00
	- Slutsyn	56,00

Dessa avgifter uppbärs i samband med byggnadslovsavgifterna, men erläggs till räddningsmyndigheten.

8 §**Övriga avgifter**

8.1	Utstakning av byggnadsplats (varvid samtliga kostnader erlägges av sökande, ingår ej i punkterna 1 - 4 i § 2).	120,73
8.2	72 § plan- och byggnadslagen för landskapet Åland avsett hörande av granne	68,61

Ersättning uppbärs även i det fall att tillstånd eller byggnadslov inte beviljas, om kommunen hört granne med stöd av stadgandena i plan- och byggnadslagen

9 §**Avgifter för avloppsanläggningar**

9.1	Avloppsanläggning för WC och BDT vatten, 1 - 5 personer	223,14
9.2	Avloppsanläggning för WC och BDT vatten, 6 - 25 personer	446,00
9.3	Avloppsanläggning för BDT vatten, 1 - 5 personer	147,02
9.4	Partiell ombyggnad av avloppsanläggning	147,02

Denna avgift debiteras skilt om den inte kan debiteras i samband med byggnadslovsavgifterna.

10 §**Inspektion av samlingslokaler**

	Inspektion och godkännande av samlingslokaler enligt samlingslokalens sammanlagda yta, per lokal	71,71
	därtill enligt lokalens sammanlagda yta (per m ²)	0,32

Taxa €**11 §**

Återbäring av avgift

Då ett byggnadslov eller något annat tillstånd förfallit eller byggherren avstår från byggnadslovet eller tillståndet medan det ännu är i kraft, återfår tillståndsinnehavaren 50 % av de avgifter han betalat.

Dock innehålles handläggningsavgifter enligt följande

- | | |
|------------------------|--------|
| - för byggnadslov | 176,49 |
| - för övriga tillstånd | 68,94 |

Om byggnadsarbetet påbörjats ges ingen återbäring.

12 §

Avslag på ansökan

Om en ansökan om tillstånd avslås eller sökande annullerar ansökan innan beslutet meddelats, men beslutsförslaget redan beretts, uppbärs 50 % av avgiften i denna taxa.

13 §

Grunder för avgiften

Då avgiften fastställs inberäknas i byggnadens totala yta, våningarnas, källarens och vindsutrymmets sammanlagda ytor, utgående från det yttre måttet. Man räknar inte med balkonger, skyddstak eller utrymmen med en rumshöjd lägre än 160 cm.

14 §

Taxans ikraftträdande

Denna taxa gäller från den 1.1.2025

Byggnadstillsynsavgiften och övriga avgifter i denna taxa faktureras enligt gällande taxa den dag beslutet fattats.

Familjestorlek	Nedre inkomstgräns euro/mån	Avgiftsprocent (räknas på överstigande del)	Inkomst som ger maxavgift, 240 euro
2 personer	1 248,-	11,5	3 334,96
3 personer	1 456,-	9,4	4 009,20
4 personer	1 664,-	7,9	4 701,98
5 personer	1 872,-	7,9	4 909,98
6 personer	2 080,-	7,9	5 117,98

Familjebegreppet = Den eller de vårdnadshavare som lever samman med barnet. I familjen inräknas även den som vårdnadshavaren stadigvarande i äktenskap eller under äktenskapsliknande former har gemensamt hushåll med och som inte är barnets vårdnadshavare i det fall barnet sammanlever med endast en vårdnadshavare. Dessutom räknas de barn för vilka dessa är underhållsskyldiga om de bor i samma hushåll.

Avgift för daghem och familjedagvård

Maxavgift: 240 euro, heltid (100%), 200 timmar/månad
192 euro, deltid (80 % av heltidavgift), 160 timmar/ månad
144 euro, halvtid (60 % av heltidsavgift), 120 timmar/ månad

Syskonrabatt: Per barn för 100 %- plats: 25€/månad
Per barn för deltidsplats: 20€/månad
Per barn för halvtidsplats: 15€/månad
För fritidshemsbarn: 10€/månad

Förundervisningen (5 h/verksamhetsdag,25h/vecka) är avgiftsfri läsåret innan barnet börjar grundskolan. Avgiftsfriheten gäller alla dagar från grundskolans hösttermins start till grundskolans vårterminsslut. Förundervisningen motsvarar en halvtidsplats (60 %). Avgift för resterande barnomsorg enligt fastställd taxa.

Maxavgiften för barn i förundervisningen:

- Heltid (100%) 144€/månad (60% av heltidavgift)
- Deltid (80%) 60€/månad (25 % av heltidavgift)
- Halvtid (60%) avgiftsfri

För barn med skoluppskov debiteras ingen avgift.

En månadsavgift som är mindre än 10€ debiteras inte.

För barnomsorg som ges i habiliterande syfte enligt landskapslagen (1978:48) om tillämpning av lagen angående specialomsorger om utvecklingsstörda och för specialfritidshem debiteras ingen avgift.

Avgift erläggs för 11 månader/år om man under en sammanhängande period om minst 4 veckor inte nyttjar barnomsorg. Ytterligare en avgiftsfri månad kan erhållas om man under tidsperioden vecka 24 t.o.m. vecka 34, under en sammanhängande tidsperiod om 8 veckor, inte nyttjar barnomsorg.

Barnomsorgsavgifterna baserar sig på bestämmelserna i landskapslagen om barnomsorg och grundskola (ÅFS 2020:32) samt på kommunfullmäktiges beslut.



Avgiftstillämpning inom barnomsorgen i Lemland och Långsunds kommuner

Avgift för plats på daghem, fritidshem eller i familjedagvård bestäms enligt familjens storlek och inkomst och betalas i form av en månadsavgift. Avgiften fastställs för ett verksamhetsår i taget. Avgift uppbärs för 11 månader/år om man under en sammanhängande period om minst 4 veckor inte nyttjar barnomsorg. Ytterligare en avgiftsfri månad kan erhållas om man under tidsperioden vecka 24 t.o.m. vecka 34, under en sammanhängande tidsperiod om 8 veckor, inte nyttjar barnomsorg.

För förundervisning under minst 4 timmar per arbetsdag under läsåret innan barnet börjar grundskolan eller får motsvarande undervisning på annat sätt uppbärs ingen avgift. Avgiftsfriheten gäller alla dagar från grundskolans höstterminsstart till grundskolans vårterminsslut.

Inkomstuppgifter för fastställelse av barnomsorgsavgift

Då avgiften fastställs skall familjens alla fortlöpande skattepliktiga och skattefria inkomster beaktas. Dit räknas

- alla löneinkomster av huvud- och bisysslor
- alla typer av pensioner
- inkomster av självständig yrkesutövning och företagsverksamhet
- kassaunderstöd
- underhållsbidrag och stöd
- alla kapital-, ränte-, dividend- och hyresinkomster
- dagpenning via FPA

Som inkomst beaktas inte barnbidrag, vårdbidrag för barn, hemvårdsstöd för barn, bostadsbidrag, studiestöd eller andra understöd som erlaggs p.g.a. studier. Som inkomstavdrag räknas underhållsbidrag som familjen betalar.

Inkomster måste verifieras med löneintyg/lönespecifikation. Om lönen är oregelbunden ska intyget förutom senaste löneperiod även visa uppgift över de senaste 6 månaderna. Egen företagare lämnar in förskottsintehållningsbevis, bokslutsuppgifter eller annat som klargör inkomstnivån.

Beskattningsintyg över senast verkställda beskattning ska bifogas inkomstintygen.

Semesterpenningens storlek bör framgå av intyget. Då uppgift om semesterpenningens storlek saknas på löneintyget beaktas en semesterpenning motsvarande 6 % av lönen.

Uppgifter om familjens inkomst lämnas till barnomsorgskansliet, både för nya och gamla barnomsorgstagare, inom augusti månad. Om inkomstuppgifterna inkommer senare korrigeras inte barnomsorgsavgiften retroaktivt. Avgiften fastställs för ett verksamhetsår i gången.

I de fall barnomsorgsplatsen tas i bruk under pågående verksamhetsperiod ska utredning om inkomsterna göras efter det att dagvården inletts.

Om familjen inte lämnar in en utredning över sina inkomster inom utsatt tidpunkt debiteras maxavgift.



Avgift under inskolningsperiod

I erhållen barnomsorgsplats ingår en veckas avgiftsfri inskolning av barnet i kommunen. För att närvaron vid dagvårdsplatsen skall räknas som inskolning bör förälder eller någon annan för barnet närstående person vara med. Inskolning bör ske veckan innan barnomsorgsplatsen tas i bruk. Undantag från detta beviljas endast av särskilda skäl. Inskolning kan ske under längre tid än en vecka men skall då försiggå under normal avgiftsbelagd dagvårdstid.

Frånvaro som påverkar avgiften

- Om barnet är frånvarande minst tio verksamhetsdagar p.g.a. sjukdom under en kalendermånad debiteras en halv månadsavgift.
- Om barnet är frånvarande en hel kalendermånad p.g.a. sjukdom debiteras ingen avgift.
- Om barnet är frånvarande en hel kalendermånad av annan orsak, debiteras en halv månadsavgift.
- Om vårdnadshavarna själva kan ordna vården under barnomsorgens planeringsdagar är de dagarna avgiftsfria.
- Avgift uppbärs inte under den tid föräldrapenningsdagar tas ut för barnet, om vårdnadshavaren meddelat kommunen detta enligt följande:

Ett regelbundet uttag av högst fem föräldrapenningsdagar för barnet ska meddelas kommunen senast två veckor före den första föräldrapenningsdagen tas ut. Ett uttag av mer än fem föräldrapenningsdagar i följd för barnet ska meddelas kommunen senast sex veckor före perioden börjar. Meddelande om uttag av föräldrapenningsdagar ska göras skriftligt.

Vid uttag av föräldrapenningsdagar får inte barnomsorgsplats nyttjas. Vid uttag av föräldrapenningsdagar har barnet rätt till samma barnomsorgsplats under en sammanhängande tid om högst 13 veckor.

Val av vårdkategori/vårdtid

Vårdtiden görs upp mellan barnets vårdnadshavare och vårdplatsens föreståndare då barnomsorgsplatsen tas i bruk. Vid val av reducerad vårdtid ansvarar vårdnadshavarna för att i tvåveckorsperioder förhandsboka barnets vårdtider. Uteblivna förhandsbokningar innebär automatiskt heltidsavgift. En överskridning av medelveckovårdtiden faktureras enligt en högre kategori för ifrågasvarande månad. Observera att bokad tid = förbrukad tid.

- Heltidsplats - ger vårdnadshavare rätt att använda barnomsorg 200 timmar/ månad
- Deltidsplats (25-35h/vecka) - ger vårdnadshavare rätta att använda barnomsorg 160 timmar/ månad
- Halvtidsplats - ger vårdnadshavare rätt att använda barnomsorg 120 timmar/ månad



Ändringar i vårdtider

Ändring av vårdkategori görs senast två veckor innan vårtiden ska ändras i Wilma eller med blanketten för ändring av vårdtid. Avgiften ändras från och med början av den månad där ändringen sker. Blanketten finns på Lemlands kommuns hemsida > blanketter. Ändring av deltidsp plats eller halvtidsp plats ska gälla för en längre tid, utgångspunkten är minst 2 månader. Meddela även daghemmets föreståndare senast 2 veckor innan ändring av vårdtid sker.

Ändring av inkomster

Om familjens inkomster förändras väsentligt, minst 10 procent och/eller varaktigt under året ska detta meddelas barnomsorgskansliet så att avgiften kan justeras. Om man underlåter sig att lämna in inkomstuppgifter kan avgiften korrigeras retroaktivt.

Uppsägning av dagvårdsplats

Uppsägning av dagvårdsplats görs skriftligt senast två veckor innan behovet av plats upphör. Blankett finns på Lemlands kommuns hemsida > blanketter och lämnas till barnomsorgskansliet. Då barnet börjar eller slutar mitt i en månad betalas avgift för en del av månaden.

Fritidshemstaxa

Dnr: 267/2024

Antagen av kommunfullmäktige genom § xx/xx.11.2024 att gälla från 1.1.2025.

Avgiften för en fritidshemsplats bestäms enligt familjens storlek och inkomst. Familjen ska årligen lämna in intyg över sina inkomster.

Beskattningsintyg över den senast fastställda beskattningen ska lämnas av alla familjer. Då uppgifter om semesterpenningens storlek saknas på löneintyget beaktas en semesterpenning motsvarande 6 procent av lönen.

Om man inte lämnar in intyg eller om intygen är ofullständigt ifyllda debiteras högsta fritidshemsavgift.

Familjestorlek	Nedre inkomstgräns euro/mån	Avgiftsprocent (räknas på överstigande del)	Inkomst som ger maxavgift
2 personer	1 248,-	11,5	3 334,96
3 personer	1 456,-	9,4	4 009,20
4 personer	1 664,-	7,9	4 701,98
5 personer	1 872,-	7,9	4 909,98
6 personer	2 080,-	7,9	5 117,98

Familjebegreppet = Den eller de vårdnadshavare som lever samman med barnet. I familjen inräknas även den som vårdnadshavaren stadigvarande i äktenskap eller under äktenskapsliknande former har gemensamt hushåll med och som inte är barnets vårdnadshavare i det fall barnet sammanlever med endast en vårdnadshavare. Dessutom räknas de barn för vilka dessa är underhållsskyldiga om de bor i samma hushåll.

Avgift för fritidshem

Maxavgift: 170 euro per barn och månad.

Avgiften är för det yngsta barnet i familjen.

Syskonrabatt: 25 euro per barn för heltidsplats inom barnomsorgen
20 euro per barn för deltidsplats inom barnomsorgen
15 euro per barn för halvtidsplats inom barnomsorgen
10 euro per barn för fritidshemsplats.

För familjer med inkomster under avgiftstaxans nedre inkomstgräns fastställs avgiften till 0 euro.

Fritidshemsavgiften baserar sig på bestämmelserna i landskapslagen (2020:32) om barnomsorg och grundskola samt på kommunfullmäktiges beslut.

Avgift under skollov

Under skolloven erbjuds fritidshemsverksamhet under de tider som daghemmet är öppet och har verksamhet. Om daghemmet inte har barn i barnomsorg under ett lov ordnas inte fritidshemsverksamhet.

Behov av fritidshemsverksamhet under skollov ska meddelas till enheten.

Vårdnadshavare ska skriftligen meddela behov av fritidshemsplats under sommaren senast 30 april till bildningsförvaltningen.

Har du bokat fritidshem men väljer att inte nyttja platsen faktureras enligt fastställd taxa.



MÅLTIDSSERVICE		Euro utan moms
Matportion inklusive transport hem. Vårdbehovsbaserad service.		8,15 €
Matportion för pensionärer från kommunen som äter på Kapellhagen		7,15 €
Matportion för pensionärer från kommunen som hämtar portion från Kapellhagen.		7,15 €
KLÄDVÅRDSSERVICE		
Tjänsten är vårdbehovsbaserad.		3,50 € /tillfälle
BAD/DUSCH SERVICE		
Pensionär / barnfamilj som badar/duschar på Kapellhagen per person / per gång utgående från vårdbehov.		3,70 € / tillfälle / person
DAGVÅRDSVERKSAMHET PÅ KAPELLHAGEN		
Inkluderar måltid, kaffe och aktiviteter. För de pensionärer som har hemserviceavgift debiteras enbart avgift för måltider.		10,80 € / tillfälle
TRYGGHETSTELEFON		
Kommunen bekostar installation av trygghetstelefon och nyckelskåp. Abonnetten debiteras 37,20 €/månad av telefonoperatören. Om klienten förstör eller tappar bort sitt larm debiteras klienten en självriskandel om 59 €.		37,20 € / månad 59 € / tillfälle
ÖVRIGA AVGIFTER		
Hemtransport av matkasse från närbutik. Vårdbehovsbaserad service.		5,40 € / tillfälle
Hemtransport av medicin. Vårdbehovsbaserad service.		5,40 € / tillfälle
Medåkning/skjuts till närbutik/Kapellhagen. Vårdbehovsbaserad service.		5,40 € /tur och retur
Avgift periodplats. Gäller ej avlastning för närståendevårdaren.		26,40 € /dygn
Avgift för oanvänd service. Exempelvis frånvaro från periodavlastning utan att meddela sig. Tillämpas ej vid akut sjukdomsfall.		59,60 € / tillfälle
Avgift för tillfälliga hembesök, exempelvis trygghetsalarmering och sjukvårdsuppgifter inom ramen för sammanhållen hemvård.		10,20 € /30 min



HEMSERVICEAVGIFTER FÖR KLIENTER I KOMMUNEN 2025

Dnr: 268/2024

Avgiften för fortlöpande och regelbunden hemservice beräknas i enlighet med vad som bestäms i Landskapslag (2022:91) om klientavgifter inom socialvården. Avgifterna kan komma att justeras under året utifrån kommande indexjusteringar och lagändringar.

Den avgift som tas ut för servicen får inte överskrida kostnaderna för serviceproduktionen.

Månadsavgiften för fortlöpande och regelbunden hemservice bestäms utifrån antalet servicetimmor som skrivits in i servicebeslutet, klientens betalningsförmåga och familjens storlek.

Avgift för fortlöpande och regelbunden hemservice avser hemservice som sker minst en gång i veckan och servicen dessutom beräknas pågå i minst två månader då den inleds eller redan har pågått i minst två månader.

Landskapsregeringen har fastställt att den högsta procentsatsen för ett hushåll med **en person är 35 %** av de inkomster som överstiger inkomstgränsen. Den högsta procentsatsen för familjer med **två personer är 24 %** av de inkomster som överstiger inkomstgränsen.

Inkomstgränserna är följande:

Antal personer i familjen	Inkomstgräns i euro per månad
1	653
2	1205
3	1891
4	2338
5	2830
6	3251

Om familjen består av fler än sex personer höjs inkomstgränsen med 363 euro för varje därpå följande familjemedlem.

Betalningsprocenttalen är följande:

Servicetimmor per månad	Betalningsprocenttal enligt familjens storlek					
	1	2	3	4	5	6 eller fler
4 eller färre	8,00	7,00	6,00	6,00	6,00	6,00
5	10,00	8,75	7,50	7,50	7,50	7,50
6	12,00	10,50	9,00	9,00	9,00	9,00
7	14,00	12,25	10,50	10,50	10,50	10,50
8	16,00	14,00	12,00	12,00	12,00	12,00
9	17,00	14,75	12,50	12,50	12,50	12,00
10	18,00	15,50	13,00	13,00	13,00	12,00
11	19,00	16,25	13,50	13,50	13,50	12,00
12	20,00	17,00	14,00	14,00	14,00	12,00
13	21,00	17,75	14,50	14,50	14,00	12,00

14	22,00	18,50	15,00	15,00	14,00	12,00
15	23,00	19,25	15,50	15,50	14,00	12,00
16	24,00	20,00	16,00	16,00	14,00	12,00
17	24,50	20,50	16,50	16,00	14,00	12,00
18	25,00	21,00	17,00	16,00	14,00	12,00
19	25,50	21,50	17,50	16,00	14,00	12,00
20	26,00	22,00	18,00	16,00	14,00	12,00
21	26,50	22,50	18,50	16,00	14,00	12,00
22	27,00	23,00	19,00	16,00	14,00	12,00
23	27,50	23,50	19,00	16,00	14,00	12,00
24	28,00	24,00	19,00	16,00	14,00	12,00
25	28,50	24,00	19,00	16,00	14,00	12,00
26	29,00	24,00	19,00	16,00	14,00	12,00
27	29,50	24,00	19,00	16,00	14,00	12,00
28	30,00	24,00	19,00	16,00	14,00	12,00
29	30,50	24,00	19,00	16,00	14,00	12,00
30	31,00	24,00	19,00	16,00	14,00	12,00
31	31,50	24,00	19,00	16,00	14,00	12,00
32	32,00	24,00	19,00	16,00	14,00	12,00
33	32,50	24,00	19,00	16,00	14,00	12,00
34	33,00	24,00	19,00	16,00	14,00	12,00
35	33,50	24,00	19,00	16,00	14,00	12,00
36	34,00	24,00	19,00	16,00	14,00	12,00
37	34,50	24,00	19,00	16,00	14,00	12,00
38 eller fler	35,00	24,00	19,00	16,00	14,00	12,00

Den avgift som fastställts för servicen och som bestämts utifrån en persons betalningsförmåga kan nedsättas eller efterskänkas till den del förutsättningarna för personens eller familjens försörjning eller förverkligandet av personens lagstadgade försörjningsplikt äventyras av att avgiften tas ut.

Nedsättning eller efterskänkning av klientavgiften baseras på en individuell bedömning av situationen.

Bestämmande och justering av avgift

Kommunen fattar ett avgiftsbeslut som gäller tills vidare. Avgiften ska emellertid justeras på ansökan av klienten eller klientens företrädare eller på initiativ av kommunen om:

- 1) Klientens eller dennes familjs inkomster har förändrats
- 2) Klientens eller dennes makes eller sambos rätt till avdrag (enligt lagstiftning) har förändrats.
- 3) Familjens förhållanden har förändrats.
- 4) Avgiften visar sig vara felaktig.
- 5) Den klientplan som utarbetats för klienten ändras så att den påverkar storleken på klientavgiften.
- 6) Kommunens betalningsgrunder ändras så att det påverkar storleken på klientavgiften.



AVGIFTER FÖR SERVICEBOENDE MED HELDYGNSOMSORG 2025

Dnr: 268/2024

HYRESAVGIFT FÖR LÄGENHET PÅ KAPELLHAGEN						
Lägenhetshyrorna är fastställda till 11 €/m² vilket inkluderar el, värme, vatten, fri bastu och avfallshantering samt tillgång till biltak med motorvärmare och till de gemensamma utrymmena.						
Hyra enligt lägenhetsnummer:						
LÄG.NR	M ²	EURO		LÄG.NR	M ²	EURO
1	40,5	445,50		7-9	33,5	368,50
2	34,5	379,50		10	45,5	500,50
3-5	33,5	368,50		11	57,5	632,50
6	40,5	445,50				

Hyra vid långvarigt serviceboende med heldygnssorg

Vid långvarigt serviceboende med heldygnssorg tecknas ett hyresavtal. Hyreskostnaden är separat och ingår ej i avgiften för serviceboende med heldygnssorg. Hyreskostnaden dras av vid uträkning av avgift för långvarigt serviceboende med heldygnssorg enligt de exempel som anges sist i dokumentet.

Ifall klienten erhåller bostadsbidrag dras summan av från boendeutgifterna vid uträkning av avgift för långvarigt serviceboende med heldygnssorg.

Avdrag vid långvarigt serviceboende med heldygnssorg.

Som avdrag från inkomsterna för beräkning av avgiften beaktas:

- Underhållsbidrag och andra motsvarande kostnader som orsakas av de faktiska familjeförhållandena (avdrag görs inte om mottagaren av bidraget är make till klienten och makarna har levt i gemensamt hushåll omedelbart innan servicen inleddes).
- Gottgörelse som förordnats av en skiftesman eller domstol enligt lagen om upplösning av sambos gemensamma hushåll (FFS 26/2011) som klienten ska betala.
- Förmån som klienten ska betala i pengar och som i samband med överlåtelse av en fastighet har förbehållits för viss tid eller på livstid.
- Grundavgift som ingår i en intressebevakares arvode

Avdrag för tidigare boendekostnader

Vid inflyttning till permanent boendeplats finns möjlighet för klienten att göra avdrag för tidigare nödvändiga och skäligena bostadskostnader enligt följande alternativ;

- 1) I fråga om ägarbostad de nödvändiga och skäligena kostnaderna för bostaden under de senaste 6 månaderna. Avdragen görs så länge kostnaderna finns kvar eller max 6 månader.
- 2) Hyran för en hyresbostad och övriga nödvändiga och skäligena kostnader för boendet under hyresgästens uppsägningstid enligt 46 § i hyreslagen (1999:19) för landskapet Åland.
- 3) Det bruksvederlag för tre månader för en bostadsrättsbostad som avses i 32 § i lagen om bostadsrättsbostäder (FFS 393/2021) och övriga nödvändiga och skäligena kostnader för boendet.

Nödvändiga och skäliga avgifter är kostnader för till exempel el, värme, vatten och försäkringar. Avdragen avser klientens faktiska kostnader, ifall klienten bott tillsammans med en partner dras kostnaderna av till hälften.

Avgift för långvarigt serviceboende med heldygnsomsorg

Kommunen debiterar avgift för långvarig service som ges på serviceboende med heldygnsomsorg om servicen beräknas pågå i minst tre månader då den inleds eller redan har pågått i minst tre månader.

Avgiften för långvarigt serviceboende med heldygnsomsorg är 85 procent av klientens nettomånadsinkomst efter lagstadgade särskilda avdrag för till exempel läkemedelskostnader och hyra. Om klienten har högre inkomster än sin make, beaktas makens inkomst vid fastställandet av klientavgiften. Då är klientavgiften 42,5 procent av makarnas sammanlagda nettoinkomster efter de lagstadgade avdragen.

Om klienten har lägre inkomster än maken, beaktas makens inkomst inte vid fastställandet av klientavgiften. Om klientavgiften baserat på makarnas sammanlagda månatliga inkomster är större än klientavgiften baserat på klientens egna inkomster, tillämpas den avgift som baserar sig på enbart klientens inkomster.

Minst 250 euro lämnas för klientens personliga bruk per månad. I avgiften för serviceboende med heldygnsomsorg ingår:

- Klädservice, veckostädning, tvätt- och städmedel,
- Vård och omsorg dygnet runt
- Trygghetslarm
- Måltider

Vid boende på serviceboende med heldygnsomsorg bekostar klienten själv hälso- och sjukvård, hjälpmedel, frisör, fot- och tandvård, hygienartiklar och kläder.

Maxserviceavgift: 6000 €/månad

Anmälan om läkemedelskostnader

Klientens läkemedelskostnader för mediciner, kliniska näringspreparat och bassalvor beaktas som ett särskilt avdrag i klientavgiften för långvarigt serviceboende med heldygnsomsorg. Det särskilda läkemedelsavdraget tas ut från de avgiftsgrundande inkomsterna för klientavgiften. I klientavgiften beaktas två särskilda läkemedelsavdrag:

- Du behöver inte ansöka om avdrag från klientavgiften för de läkemedelskostnader som ersätts enligt sjukförsäkringslagen, eftersom de beaktas automatiskt upp till avgiftstaket när klientavgiften fastställs. För år 2024 är den totala årssjälvriskan 626,94 €/år vilket motsvarar 52,25 €/månad.
- Du ska ansöka om avdraget för de läkemedelskostnader som inte ersätts enligt sjukförsäkringslagen med en separat ansökan. Läkemedelskostnader som inte ersätts enligt sjukförsäkringslagen beaktas i klientavgiften till den del som en yrkesutbildad person inom hälso- och sjukvården har konstaterat dem vara nödvändiga.

Uträkning av avgift för serviceboende med heldygnsomsorg

Exempel 1

Månadsinkomst:

- Pension, 2113,68 €
- Vårdbidrag för pensionstagare, 362,62 € Total månadsinkomst, 2476,30 €

Avdrag:

- Medicinkostnad, 52,25 €
- Hyra (belopp minskat med bostadsbidrag), 330,44 €

Total kostnad för avdrag 382,69 €

Klientavgift:

- $2476,30 \text{ € (månadsinkomst)} - 382,69 \text{ € (avdrag)} = 2093,61 \text{ €}$
- $2093,61 \text{ €} \times 0,85 = \mathbf{1779,57 \text{ €}}$

Kvar till förfogande:

- $2093,61 \text{ € (månadsinkomst - avdrag)} - 1779,57 \text{ € (klientavgift)} = \mathbf{314,04 \text{ €}}$

Minimibelopp för personligt bruk 250 €/månad

Lumparlands skolas hyrestaxor 1.1.2025

Lumparlands grundskola	Hyresbelopp exkl moms 1.1.2024	Ny avgift fr.o.m 1.1.2025 inkl moms	Hyresbelopp exkl moms 1.1.2025	Avgift fr.o.m 1.1.2024 inkl moms	Prisjustering i euro	Moms	Moms	Förhöjnings %	Ny avgift fr.o.m 1.1.2025 inkl moms
						10 %	25,5 %	2,00 %	
Klassrum (kväll 4 h)	19,07	24,41	19,45	23,65	0,76		4,96	0,47	24,41
Gymnastiksal (4 h)	21,48	24,10	21,91	23,63	0,47	2,19		0,47	24,10
Gymnastiksal (1 h)	5,63	6,32	5,74	6,19	0,12	0,57		0,12	6,32
Dusch och omklädningsrum	8,22	9,22	8,38	9,04	0,18	0,84		0,18	9,22
Matsal (½ dag eller kväll 4 h)	19,07	24,41	19,45	23,65	0,76		4,96	0,47	24,41
Kök (½ dag eller kväll 4 h)	19,07	24,41	19,45	23,65	0,76		4,96	0,47	24,41
Matsal och kök (½ dag eller kväll 4 h)	38,56	49,36	39,33	47,81	1,55		10,03	0,96	49,36
Matsal (heldag)	38,56	49,36	39,33	47,81	1,55		10,03	0,96	49,36
Kök (heldag)	38,56	49,36	39,33	47,81	1,55		10,03	0,96	49,36
Matsal och kök (heldag)	78,64	100,67	80,21	97,51	3,15		20,45	1,95	100,67
Slöjdsal, textilsal (kväll 4 h)	19,07	24,41	19,45	23,65	0,76		4,96	0,47	24,41
Slöjdsal, trä- och metall (kväll 4 h)	19,07	24,41	19,45	23,65	0,76		4,96	0,47	24,41

Kommunen har en mycket restriktiv hållning vad gäller att hyra ut skolan för övernattnings. Endast i sådana fall där skolan har haft kontakt med andra skolor och elever är det möjligt att vid kontakter och utbyte upplåta skolan för övernattnings. I dylika fall erläggs ingen avgift. Utbildningsnämnden får i undantagsfall avvika från taxorna vid större evenemang eller för sådana tillställningar som är speciellt viktiga för kommunen eller landskapet Åland. Ingen städning ingår i hyran.

SNÖPLOGNINGSAVGIFT 1.10.2025-30.4.2026**Lumparland**

Godkänd av kommunfullmäktige xx.xx.xxxx §

Denna grundavgift tillämpas för plogningsarbete som utförs under perioden 1.10.2025 till 30.4.2026.

Infartslängd	Exkl.moms	Inkl.moms Infart	Inkl.moms Uppsamlingsväg
0-250 meter	172,84 €	216,92 €	433,84€
251-500 meter	224,69€	281,99€	563,98€
501-1000 meter	311,11€	390,45€	780,89€
1001-1500 meter	414,82€	520,60€	1041,20€
1501-2000 meter	561,72€	704,96€	1409,92€
2001-∞ meter	795,08€	997,82€	1995,64€

Avgifterna debiteras med stadgad mervärdesskatt (25,5%).

Beställer man snöplogning efter 1.10.2025 tillkommer en behandlingsavgift om 50 €.

Snöplogningen fungerar enligt följande:

1. Anhållan om snöröjning bekräftas genom inbetalning av fakturerad föreskriven avgift senast vid periodens början. Anhållan skickas till Lemlands kommun / tekniska avdelningen.
2. Målsättningen är att vägen skall vara framkomlig med personbil. Vid ymnigt snöfall, snöstorm eller annan exceptionell väderlek kan detta dock inte garanteras.
3. Vägen måste vara i sådant skick att den går att ploga med traktor och plog. Detta betyder bl a att vägen är röjd, tillräckligt plan samt utmärkt med plogpinnar i tillräckligt antal.
4. Vändplan bör finnas för traktor och plog.
5. Privatvägarna indelas i infarter och uppsamlingsvägar
Infart = en privat väg som används endast av ett hushåll
Uppsamlingsväg = en privat väg som används av minst tre hushåll. Uppsamlingsvägen behöver inte sammanfalla med ”väglagsvägen”. Uppsamlingsväg som används av två hushåll likställs med privat infart och betalas i samband med privat infart.
6. I första hand plogas uppsamlingsvägar. Plogningen av dessa beställs av väglag eller privatpersoner. Uppsamlingsvägens längd mäts mellan allmän väg/en annan uppsamlingsväg och det näst sista hushållets avtag om inte annat överenskomms med väglaget.
7. Plogas uppsamlingsvägen av kommunen kan också infarter plogas. Plogningen av dessa beställs av privatpersoner. Infartens längd mäts mellan uppsamlingsvägen och hushållets gårdsplan.
8. Avgiften för plogning av uppsamlingsvägar är 2 x summan angiven i snöplogningsavgiften
9. Avgiften för plogning av privata infarter är den i avgiften angivna

Avloppsvattentaxa Lumparland År 2025

Kommunen har ett allmänt avloppsverk som emottar avloppsvatten för vidare transport från abonnenten till reningsverket i Mariehamn. För att täcka våra kostnader uppbärs avgifter i form av anslutningsavgifter samt förbrukningstaxor för dessa tjänster.

Verksamheten regleras av LL om allmänna vatten- och avloppsnät samt LL om avloppsvattentaxa. Enligt LL om ändring av 5 § i lagen om avloppsvattenavgift (ÅFS 56/05) ”*skall bruksavgiften senast den 31.12.2010 på grund av den mängd vatten som används i fastigheten fastställas så att avgiften täcker kostnaderna för vattentjänsten*”. Lagen trädde i kraft den 1.1.2006. Sedan 2018 är avskrivningarna med i budgeten för att ge en korrekt bild av kostnaderna.

Till kommunens avloppsnät är i dagens läge ca 410 fastigheter anslutna.

Taxa innefattande detaljerade grunder för fastställande av avloppsvattenavgift godkänns av kommunens fullmäktige.

Lotsbroverket kommer att höja sin taxa för avloppsvatten med 3% inför 2025.

	BS2022	BS2023	BU2024	BU2025
Ext. Utg	-43650	-44269	-51672	-52350
Ext. Ink	64 429	74360	74697	75550
Int. Utg	-29 309	-39854	-32605	-31650
Int. Ink	8 530	9764	9580	9880
Avskrivn.	-6 740	-7075	-7075	-6742
Netto	-6740	-7074	-7075	-5312

Till Ålands lagting

Landskapslag om cybersäkerhet och motståndskraft

Huvudsakligt innehåll

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

Syftet med lagförslaget är att inom landskapet genomföra Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) samt Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Avsikten är att den föreslagna landskapslagen ska träda i kraft den

INNEHÅLL	
Huvudsakligt innehåll	1
Allmän motivering	3
1. Inledning	3
2. Nuläge	4
2.1 Det gamla cybersäkerhetsdirektivet (NIS 1-direktivet).....	4
2.2 Cybersäkerhetsdirektivet (NIS 2-direktivet).....	5
2.3 Direktivet om kritisk infrastruktur	15
2.4 Motståndskraftsdirektivet (CER-direktivet)	16
2.5 Den allmänna dataskyddsförordningen	31
2.6 Kodexdirektivet.....	32
2.7 Komparativ utblick	34
2.8 Sammanfattande bedömning	38
3. Landskapsregeringens förslag och syften	39
4. Lagstiftningsbehörighet.....	41
4.1 Allmänt	41
4.2 De digitala sektorerna	44
4.3 Cybersäkerhetsdirektivet	48
4.4 Motståndskraftsdirektivet	49
5. Förslagets verkningar	51
5.1 Allmänt.....	51
5.2 Ekonomiska verkningar.....	52
5.3 Verkningar för myndigheterna	52
5.4 Övriga samhällsliga verkningar.....	54
6. Ärendets beredning	54
Detaljmotivering	54
Landskapslag om cybersäkerhet och motståndskraft	54
Lagtext	97
L A N D S K A P S L A G om cybersäkerhet och motståndskraft.....	97

Allmän motivering

1. Inledning

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, Europaparlamentet 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 (cybersäkerhetsdirektivet), även kallat NIS 2-direktivet (efter engelskans *Network and Information Systems Directive*), och Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (motståndskraftsdirektivet), även kallat CER-direktivet (efter engelskans *Critical Entities Resilience Directive*).

Cybersäkerhetsdirektivet ersätter det gamla cybersäkerhetsdirektivet från 2016. Cybersäkerhetsdirektivets syfte är att genom fastställande av åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen förbättra den inre marknadens funktion. Cybersäkerhetsdirektivet utvidgar tillämpningsområdet och kravställningen på berörda verksamhetsutövare och samarbetsformer i förhållande till det gamla cybersäkerhetsdirektivet.

Mostståndskraftsdirektivet är helt nytt och dess syfte är att bidra till säkerställandet av motståndskraften hos samhällskritiska verksamhetsutövare i fråga om ömsesidigt beroende tjänster, vilka är kritiska med tanke på samhällets funktionsförmåga samt upprätthålla samhällets ekonomiska funktioner.

Båda direktiven utgör minimidirektiv, med innebörden att den åländska lagstiftningen skulle kunna innehålla mer långtgående skyldigheter, vilket dock inte föreslås i detta lagförslag.

Landskapsregeringen föreslår att direktiven genomförs på Åland på miniminivån, genom omskrivningsmetoden, och föreslår att detta ska ske genom en allmän och gemensam lag, vilken tillvaratar de synergieffekter som överlappningen mellan direktivens tillämpningsområden medger.

Direktiverna föreskriver ett nationellt genomförande vilket påför utpekade myndigheter för tillsyn och andra särskilda roller ett större antal detaljerade uppgifter och skyldigheter. Regleringen av skyldigheterna för berörda offentliga och enskilda verksamhetsutövare inom de sektorer vilka faller inom regleringens tillämpningsområde är i sammanhanget mer sparsam och allmänt utformad.

De myndigheter vilka påförs särskilda roller förväntas i huvudsak att samarbeta nationellt såväl som internationellt med andra relevanta myndigheter, påförs detaljerade underrättelse- och informationsskyldigheter, bemyndigas att vidta tillsyn- och efterlevnadskontrollåtgärder och förväntas att på olika sätt stödja berörda verksamhetsutövares uppfyllnad av genomförandets kravställning.

Berörda verksamhetsutövare påförs i huvudsak skyldigheter att på egen hand eller av utpekad myndighet antingen klassificeras eller identifieras som en berörd verksamhetsutövare, till utpekad myndighet tillhandahålla relevant information i samband med detta, genomföra riskbedömningar, upprätta en plan och strategi i enlighet med riskbedömningen, erbjuda utbildning av personal, vidta ett strukturerat riskhanteringsarbete med vidtagande av relevanta riskhanteringsåtgärder och att rapportera om främst betydande incidenter till utpekade myndigheter.

2. Nuläge

2.1 Det gamla cybersäkerhetsdirektivet (NIS 1-direktivet)

2.1.1 Bakgrund och syfte

Den 6 juli 2016 antogs Europaparlamentet och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat *det gamla cybersäkerhetsdirektivet*, även kallat NIS 1-direktivet).

Syftet med det gamla cybersäkerhetsdirektivet var att förbättra den inre marknadens funktion genom att skapa tillit och förtroende och att fastställa åtgärder för att uppnå en gemensam hög nivå på säkerhet i nätverks- och informationssystem inom unionen. Flera av åtgärderna syftar till att säkerställa kontinuiteten i de samhällsviktiga och digitala tjänster som omfattas av direktivet. Målet med det gamla cybersäkerhetsdirektivet var att förbättra cybersäkerhetsberedskapen på unionens territorium och införa rapporterings- skyldighet för väsentliga verksamhetsutövare (i det gamla såväl som i det nya direktivet benämnda som entiteter) i fråga om informationssäkerhetsincidenter.

2.1.2 Genomförandet på Åland

Ålands landskapsregering bedömde vid tiden för det gamla cybersäkerhetsdirektivets genomförande att frågan föll inom ramen för rikets lagstiftningsbehörighet över televäsendet, enligt 27 § 40 punkten självstyrelselag (ÅFS 1991:71) för Åland. I dag gör Ålands landskapsregering en annan bedömning, se närmare redogörelse av lagstiftningsbehörigheten avseende cybersäkerhetsdirektivet under avsnitt 4 nedan. Oavsett genomfördes aldrig det gamla cybersäkerhetsdirektivet på Åland och de berörda verksamhetsutövarna har hittills, i varierande grad, tillämpat rikets reglering i den sektors-specifika speciallagstiftningen.

2.1.3 Genomförandet i riket

Det gamla cybersäkerhetsdirektivet genomfördes i huvudsak i riket genom lagändringar i förevarande lagstiftning, se RP 192/2017 rd, vilka trädde i kraft den 9 maj 2018. Det stiftades därmed inte någon nationell, horisontell allmän lag om informations- och nätverkssäkerheten, utan det gamla cybersäkerhetsdirektivet genomfördes genom att skyldigheterna införlivats i den sektorsspecifika speciallagstiftningen. Övervakningen av att skyldigheterna kring informationssäkerheten fullgörs splittrades därmed mellan flera sektors-specifika myndigheter.

Genomförandebestämmelserna återfinns främst i lagen om tjänster inom elektronisk kommunikation (FFS 917/2014) (nedan kallad *lagen om elektronisk kommunikation*), luftfartslagen (FFS 864/2014), spårtrafiklagen (FFS 1302/2018), lagen om fartygstrafikservice (FFS 623/2005), lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (FFS 485/2004), lagen om transportservice (FFS 320/2017), elmarknadslagen (FFS 588/2013), naturgasmarknadslagen (FFS 587/2017) och lagen om vattentjänster (FFS 119/2001).

I den sektorsspecifika lagstiftningen återfinns bestämmelser om de viktigaste tjänsteleverantörernas skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och att anmäla informationssäkerhetsincidenter till tillsynsmyndigheten och allmänheten.

Tillsynen har ordnats sektorsspecifikt, det vill säga sektorsspecifika tillsynsmyndigheter övervakar verksamhetsutövare inom respektive sektor. Riket utsåg Energimyndigheten, Transport- och kommunikationsverket, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården

(Valvira) samt Närings-, trafik- och miljöcentralen i Södra Savolax till tillsynsmyndigheter.

2.2 Cybersäkerhetsdirektivet (NIS 2-direktivet)

2.2.1 Bakgrund och syfte

Den 14 december 2022 antog Europaparlamentet och rådet cybersäkerhetsdirektivet. Det ersätter det gamla cybersäkerhetsdirektivet och skärper kraven på säkerhet i verksamhetsutövarers nätverks- och informationssystem och innehåller nya bestämmelser om ett mer långtgående samarbete inom unionen. Enligt artikel 1.1 är cybersäkerhetsdirektivets syfte att genom fastställande av åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen förbättra den inre marknadens funktion. Enligt artikel 5 är cybersäkerhetsdirektivet ett minimidirektiv, med innebörden att den åländska lagstiftningen skulle kunna innehålla mer långtgående skyldigheter.

Enligt skäl 3 har nätverks- och informationssystem utvecklats till ett centralt inslag i vardagslivet genom den snabba digitala omställningen och sammankopplingen av samhället. Denna utveckling har lett till en utvidgad hotbild och fört med sig nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga 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.

Enligt skäl 4 varierar de cybersäkerhetskrav som åläggs verksamhetsutövare som tillhandahåller tjänster eller utför verksamhet som är ekonomiskt betydelsefull avsevärt mellan medlemsstaterna avseende typen av krav och tillsynsmetod. Dessa skillnader medför extra kostnader och gör det svårt för verksamhetsutövarna att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav i en medlemsstat kommer att påverka cybersäkerhetsnivån i andra medlemsstater.

Enligt skäl 5 medför alla dessa skillnader en fragmentering av den inre marknaden, vilket kan ha en skadlig inverkan på dess funktion och påverkar tillhandahållandet av tjänster över gränserna samt nivån av cybermotståndskraft. Dessa skillnader kan också leda till att vissa medlemsstater har större sårbarhet för cyberhot, med potentiella spridningseffekter i hela unionen. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk, genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera vilka sektorer och verksamheter som omfattas av skyldigheter och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder.

Enligt skäl 6 bör upphävandet av det gamla cybersäkerhetsdirektivet samtidigt leda till att tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin, så att den ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden. I synnerhet syftar direktivet till att åtgärda bristerna i fråga om differentieringen mellan

leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, vilken har visat sig vara inaktuell eftersom den inte speglar den betydelse som dessa sektorer och tjänster har för samhälleliga och ekonomiska verksamheter på den inre marknaden.

2.2.2 Tillämpningsområde och förteckning

Enligt artikel 2.1 är direktivet tillämpligt på offentliga och enskilda verksamhetsutövare av den typ som avses i direktivets bilaga I eller II och vilka betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG, eller överstiger de trösklar för medelstora företag som avses i 1 punkten i den artikeln, och vilka tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Verksamhetsutövarna finns inom 18 sektorer som delas upp i högkritiska och andra kritiska sektorer, samt delsektorer och typer av verksamhetsutövare.

Enligt bilaga I utgör följande högkritiska sektorer:

1. Energi, med delsektorerna:
 - a) elektricitet,
 - b) fjärrvärme eller fjärrkyla,
 - c) olja,
 - d) gas och
 - e) vätgas.
2. Transporter, med delsektorerna:
 - a) lufttransport
 - b) järnvägstransport,
 - c) sjöfart och
 - d) vägtransport.
3. Bankverksamhet
4. Finansmarknadsinfrastruktur
5. Hälso- och sjukvårdssektorn
6. Dricksvatten
7. Avloppsvatten
8. Digital infrastruktur
9. Förvaltning av IKT-tjänster (mellan företag, IKT är en förkortning för informations- och kommunikationsteknik)
10. Offentlig förvaltning
11. Rymden

Enligt bilaga II utgör följande andra kritiska sektorer:

1. Post- och budtjänster
2. Avfallshantering
3. Tillverkning, produktion och distribution av kemikalier
4. Produktion, bearbetning och distribution av livsmedel
5. Tillverkning, med delsektorerna:
 - a) tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik,
 - b) tillverkning av datorer, elektronikvaror och optik,
 - c) tillverkning av elapparatur,
 - d) tillverkning av övriga maskiner,
 - e) tillverkning av motorfordon, släpfordon och påhängsvagnar, och
 - f) tillverkning av andra transportmedel.
6. Digitala leverantörer
7. Forskning

Enligt artikel 2.1 är direktivet, oavsett verksamhetsutövarnas storlek, även tillämpligt på verksamhetsutövare av en typ som avses i bilaga I eller II i följande fall:

- a) Om tjänster tillhandahålls av:

- i) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,
 - ii) tillhandahållare av betrodda tjänster, och
 - iii) registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.
- b) Om verksamhetsutövaren är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk eller samhällelig eller ekonomisk verksamhet.
 - c) Om en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa.
 - d) Om en störning av den tjänst som verksamhetsutövaren tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser.
 - e) 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 medlemsstaten som är beroende av denna verksamhetsutövare.
 - f) Om verksamhetsutövaren är en offentlig förvaltningsenhet:
 - i) på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller
 - ii) på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

Enligt artikel 2.3–4 är direktivet, oavsett verksamhetsutövarnas storlek, också tillämpligt på verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt motståndskraftdirektivet och på verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster.

Enligt artikel 2.5 får medlemsstaterna föreskriva att direktivet även ska tillämpas på offentliga verksamhetsutövare på lokal nivå och utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet.

Enligt artikel 2.6 påverkar direktivet inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

Enligt artikel 2.7 är direktivet inte tillämpligt på offentliga verksamhetsutövare som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott.

Enligt artikel 2.8 får medlemsstaterna undanta särskilda verksamhetsutövare som bedriver verksamhet på dessa områden, eller som uteslutande tillhandahåller tjänster till en offentlig verksamhetsutövare som bedriver verksamhet på dessa områden, från skyldigheterna rörande riskhantering och rapportering med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska inte heller tillsyns- och efterlevnadskontrollåtgärder tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om verksamhetsutövarna bedriver verksamhet uteslutande på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning får medlemsstaten besluta att befria dessa verksamhetsutövare också från skyldigheterna om registrering.

Enligt artikel 4 föreskrivs att, om det i sektorsspecifika unionsrättsakter föreskrivs att verksamhetsutövare ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, och dessa krav har minst samma verkan, ska de relevanta bestämmelserna i cybersäkerhetsdirektivet inte tillämpas på sådana verksamhetsutövare.

Enligt artikel 3 ska verksamhetsutövare som omfattas av direktivet delas upp i väsentliga och viktiga verksamhetsutövare. Enligt artikel 3.1 ska följande verksamhetsutövare vara väsentliga:

- a) Verksamhetsutövare av en typ som avses i bilaga I och som överstiger trösklarna för medelstora företag.
- b) Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek.
- c) Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag.
- d) Offentliga verksamhetsutövare på statlig nivå.
- e) Alla andra verksamhetsutövare av en typ som avses i bilaga I eller II som av en medlemsstat identifierats som väsentliga i enlighet med artikel 2.2 b–e.
- f) Verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt motståndskraftsdirektivet.
- g) Verksamhetsutövare som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster enligt det gamla cybersäkerhetsdirektivet, om så föreskrivs av medlemsstaten.

Enligt artikel 3.2 ska alla verksamhetsutövare av en typ som avses i bilaga I eller II och som inte är väsentliga betraktas som viktiga verksamhetsutövare. Detta inkluderar verksamhetsutövare som en medlemsstat har identifierat som viktiga i enlighet med artikel 2.2 b–e.

Enligt artikel 3.3 ska medlemsstaterna senast den 17 april 2025 upprätta en förteckning över väsentliga och viktiga verksamhetsutövare samt verksamhetsutövare som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år se över förteckningen och när det är lämpligt att uppdatera den. Medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för verksamhetsutövarna att registrera sig själva.

Enligt artikel 3.5 ska medlemsstaternas behöriga myndigheter, senast den 17 april 2025 och därefter vartannat år, underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare för varje sektor och delsektor och lämna relevant information om väsentliga och viktiga verksamhetsutövare som har identifierats, oavsett storlek.

2.2.3. Behörig myndighet och gemensam kontaktpunkt

Enligt artikel 8.1 ska varje medlemsstat utse en eller flera behöriga myndigheter med ansvar för cybersäkerhet och tillsyn. Enligt artikel 8.2 ska de behöriga myndigheterna övervaka genomförandet av direktivet på nationell nivå.

Enligt artikel 8.3 ska varje medlemsstat också utse en gemensam kontaktpunkt. Enligt artikel 8.4 ska den gemensamma kontaktpunkten utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Europeiska unionens cybersäkerhetsbyrå (*Enisa*), samt säkerställa ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

Enligt artikel 8.5 ska medlemsstaterna säkerställa att deras behöriga myndigheter och gemensamma kontaktpunkter har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt utföra de uppgifter de tilldelas och därigenom uppnå målen med direktivet.

2.2.4 *Cyberkrishanteringsmyndighet och samordnande cyberkrishanteringsmyndighet*

Enligt artikel 9.1 ska varje medlemsstat utse en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser, det vill säga cyberkrishanteringsmyndigheter. Enligt artikel 9.2 ska en medlemsstat, om den utser mer än en cyberkrishanteringsmyndighet, tydligt ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Enligt artikel 9.4 ska medlemsstaten även anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av sådana incidenter och kriser fastställs, med särskilt innehåll enligt punkterna a–f.

2.2.5 *Enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) och samordnande enhet för hantering av it-säkerhetsincidenter*

Enligt artikel 10.1 ska varje medlemsstat utse en eller flera enheter för hantering av it-säkerhetsincidenter, även förkortad som CSIRT-enhet (efter engelskans *Computer Security Incident Response Team*). Enligt artikel 12.1 ska varje medlemsstat, om den har utsett fler än en enhet för hantering av it-säkerhetsincidenter, utse en till samordnare för den samordnade delgivningen av informationen om sårbarheter och den ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan den som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara produkterna eller tjänsterna. I artiklarna 10.4–5 och 11 uppställs uttryckliga krav som enheten för hantering av it-säkerhetsincidenter ska uppfylla och uppgifter som den ska utföra. Enligt artiklarna 10.2–3 och 11.2 ska medlemsstaterna säkerställa att deras enhet för hantering av it-säkerhetsincidenter har nödvändig kapacitet för att utföra dessa uppgifter och att tillräckliga resurser anslås för att säkerställa en tillräcklig personalstyrka för att göra det möjligt för enheter för hantering av it-säkerhetsincidenter att utveckla sin tekniska kapacitet.

2.2.6 *Samarbete på nationell nivå*

Enligt artikel 13.1 ska den behöriga myndigheten, den gemensamma kontaktpunkten och enheten för hantering av it-säkerhetsincidenter i en medlemsstat, om de är separata, samarbeta när det gäller fullgörandet av skyldigheterna enligt direktivet. Enligt artikel 13.2 ska medlemsstaterna säkerställa att antingen enheten för hantering av it-säkerhetsincidenter eller den behöriga myndigheten tar emot underrättelser om incidenter, cyberhot och tillbud som lämnas enligt direktivet. Enligt artikel 13.3 ska den gemensamma kontaktpunkten informeras om de underrättelser som lämnas in. Enligt artikel 13.4–5 ska medlemsstaterna också säkerställa att den behöriga myndigheten, enheten för hantering av it-säkerhetsincidenter och den gemensamma kontaktpunkten samarbetar med bland annat brottsbekämpande myndigheter, dataskyddsmyndigheter och behöriga myndigheter enligt andra sektorsspecifika unionsrättsakter.

2.2.7 *Samarbetsgrupp för strategiskt samarbete och informationsutbyte*

Genom det gamla cybersäkerhetsdirektivet inrättades en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit.

Enligt cybersäkerhetsdirektivets artikel 14 utökas samarbetsgruppen genom att fler aktörer ges möjlighet att delta i samarbetsgruppen, som dessutom tilldelas fler uppgifter, vilka återges artikel 14.4.

2.2.8 CSIRT-nätverk

Genom det gamla cybersäkerhetsdirektivet inrättades ett nätverk för nationella enheter för hantering av it-säkerhetsincidenter att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete i unionen.

Enligt artikel 15 i cybersäkerhetsdirektivet ska nätverket ska i princip fortsätta att fungera på samma sätt, men får en del nya uppgifter, till exempel att samarbeta och utbyta information med säkerhetscentrum, även förkortad som SOC (efter engelskans *Security Operations Centre*), på regional och unionsnivå.

2.2.9 Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

Enligt artikel 16 inrättas det europeiska kontaktnätverket för cyberkriser, även förkortat som EU-CyCLONe (efter engelskans *European Cyber Crisis Liaison Organisation Network*), för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser och att säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. Enligt artikel 6.7 definieras storskalig cybersäkerhetsincident i direktivet som en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera den eller som har en betydande påverkan på minst två medlemsstater.

Enligt artikel 16.2 ska EU-CyCLONe bestå av företrädare för medlemsstaternas cyberkrisermyndigheter och i vissa fall kommissionen. Enligt artikel 16.3 ska EU-CyCLONe bland annat öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser samt samordna hanteringen och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.

2.2.10 Styrning

Enligt artikel 20.1 ska medlemsstaterna säkerställa att väsentliga och viktiga verksamhetsutövers ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som verksamhetsutövaren vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för överträdelser av den artikeln. Enligt artikel 20.2 ska medlemsstaterna också säkerställa att medlemmar i ledningsorganen är skyldiga att genomgå utbildning, och ska uppmuntra verksamhetsutövare att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på verksamhetsutövarens tjänster.

2.2.11 Riskhanteringsåtgärder för cybersäkerhet

Enligt artikel 21.1 ska medlemsstaterna säkerställa att de väsentliga och viktiga verksamhetsutövare som beskrivits i förteckningen ovan vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster. Åtgärderna ska också vidtas för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken.

Enligt artikel 21.2 ska åtgärderna baseras på en allriskansats som syftar till att skydda verksamhetsutövarens nätverks- och informationssystem och dessa systems fysiska miljö från incidenter och minst inbegripa:

- a) strategier för riskanalys och informationssystemens säkerhet,
- b) incidenthantering,

- c) driftskontinuitet,
- d) säkerhet i leveranskedjan,
- e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
- f) strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
- g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
- h) strategier och förfaranden för användning av kryptografi,
- i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
- j) användning av, när så är lämpligt, lösningar för multifaktors-autentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

Enligt artikel 21.3 ska medlemsstaterna säkerställa att verksamhetsutövare beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis. Medlemsstaterna ska också säkerställa att verksamhetsutövare är skyldiga att beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med direktivet.

Enligt artikel 21.5 ska kommissionen, senast den 17 oktober 2024, anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för åtgärderna ovan när det gäller vissa verksamhetsutövare. Kommissionen får även anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorsspecifika krav med avseende på andra verksamhetsutövare.

2.2.12 Rapporteringsskyldigheter

Enligt artikel 23.1 ska varje medlemsstat säkerställa att väsentliga och viktiga verksamhetsutövare utan onödigt dröjsmål underrättar sin enhet för hantering av it-säkerhetsincidenter eller behöriga myndighet om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster, det vill säga en betydande incident. Enligt artikel 23.3 ska en incident anses vara betydande om den har orsakat eller kan orsaka allvarliga driftstörningar för tjänsterna, ekonomiska förluster för den berörda verksamhetsutövaren eller har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

Enligt artikel 23.4 ska verksamhetsutövaren lämna följande till enheten för hantering av it-säkerhetsincidenter eller, i tillämpliga fall, den behöriga myndigheten, följande:

- a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, en tidig varning som i tillämpliga fall ska ange om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.
- b) Utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, en incidentanmälan som, i tillämpliga fall, ska uppdatera den information som avses i led a och ange en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.
- c) På begäran av en enhet för hantering av it-säkerhetsincidenter eller, i tillämpliga fall, den behöriga myndigheten, en delrapport om relevanta statusuppdateringar.

- d) Senast en månad efter inlämningen av den incidentanmälan som avses i led b, en slutrapport som ska innehålla följande:
 - i) En detaljerad beskrivning av incidenten, inbegripet dess allvarlighetsgrad och konsekvenser.
 - ii) Den typ av hot eller grundorsak som sannolikt har utlöst incidenten.
 - iii) Tillämpade och pågående begränsande åtgärder.
 - iv) I tillämpliga fall, incidentens gränsöverskridande verkningar.
- e) I händelse av en pågående incident vid tidpunkten för inlämnandet av den slutrapport som avses i led d ska medlemsstaterna säkerställa att de berörda verksamhetsutövarna tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat incidenten.

Enligt artikel 23.5 ska enheten för hantering av it-säkerhetsincidenter eller den behöriga myndigheten utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av en tidig varning lämna ett svar till den rapporterande verksamhetsutövaren, inbegripet initial återkoppling om incidenten och, på verksamhetsutövarens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. Enheten för hantering av it-säkerhetsincidenter ska tillhandahålla ytterligare tekniskt stöd om den berörda verksamhetsutövaren begär det. Om incidenten misstänks vara av brottslig art ska enheten för hantering av it-säkerhetsincidenter eller den behöriga myndigheten också tillhandahålla vägledning om rapportering av incidenten till de brottsbekämpande myndigheterna.

Enligt artikel 23.6 ska enheten för hantering av it-säkerhetsincidenter, den behöriga myndigheten eller den gemensamma kontaktpunkten, när så är lämpligt, och särskilt om incidenten berör två eller flera medlemsstater, utan dröjsmål informera andra berörda medlemsstater och Enisa om incidenten. Vid en sådan underrättelse ska verksamhetsutövarens säkerhets- och affärsintressen samt informationens konfidentialitet bevaras, i enlighet med unionsrätten eller nationell rätt.

Enligt artikel 23.8 ska den gemensamma kontaktpunkten, på begäran av enheten för hantering av it-säkerhetsincidenter eller den behöriga myndigheten, vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater. Enligt artikel 23.9 ska den gemensamma kontaktpunkten, var tredje månad, lämna en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud som rapporterats enligt direktivet.

Enligt artikel 23.10 ska enheten för hantering av it-säkerhetsincidenter eller, i tillämpliga fall, den behöriga myndigheten förse de behöriga myndigheterna enligt motståndskraftdirektivet med information om rapportering som gjorts av verksamhetsutövare som identifierats som kritiska i enlighet med det direktivet.

Enligt artikel 23.11 får kommissionen anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas enligt direktivet. Senast den 17 oktober 2024 ska kommissionen, med avseende på vissa verksamhetsutövare anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt direktivet. Kommissionen får även anta sådana genomförandeakter med avseende på andra väsentliga och viktiga verksamhetsutövare.

2.2.13 Cybersäkerhetscertifiering och standardisering

Enligt artikel 24.1 får medlemsstaterna ålägga väsentliga och viktiga verksamhetsutövare att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga verksamhetsutövaren eller upphandlats från tredje parter, som är certifierade enligt

europiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med cybersäkerhetsakten. Medlemsstaterna ska dessutom uppmuntra väsentliga och viktiga verksamhetsutövare att använda kvalificerade betrodda tjänster.

Enligt artikel 24.2 får kommissionen anta delegerade akter som anger vilka kategorier av väsentliga eller viktiga verksamhetsutövare som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en ordning för cybersäkerhetscertifiering som har antagits enligt cybersäkerhetsakten.

Enligt artikel 25.1 ska medlemsstaterna, utan att föreskriva eller gynna användning av viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2.2.14 Arrangemang för informationsutbyte om cybersäkerhet

Enligt artikel 29.1 ska medlemsstaterna säkerställa att det är möjligt för verksamhetsutövare att på frivillig basis utbyta relevant information om cybersäkerhet om sådant informationsutbyte syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter, begränsa deras inverkan eller höja cybersäkerhetsnivån. Enligt artikel 29.2 ska medlemsstaterna säkerställa att informationsutbytet sker inom grupper av väsentliga och viktiga verksamhetsutövare, och i relevanta fall, deras leverantörer och tjänsteleverantörer, vilket får ske med hjälp av arrangemang för informationsutbyte om cybersäkerhet. Enligt artikel 29.3 ska medlemsstaterna underlätta inrättandet av sådana arrangemang för informationsutbyte som avses i punkten 2. Enligt artikel 29.4 ska medlemsstaterna också säkerställa att väsentliga och viktiga verksamhetsutövare underrättar den behöriga myndigheten om sitt deltagande i sådana arrangemang.

2.2.15 Tillsyn och efterlevnadskontroll

Enligt artikel 31.1 ska medlemsstaterna säkerställa att deras behöriga myndighet på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att direktivet efterlevs. Enligt artikel 31.2 får medlemsstaterna tillåta sin behöriga myndighet att prioritera sin tillsyn utifrån en riskbaserad metod. Enligt artikel 31.3 ska den behöriga myndigheten ha ett nära samarbete med tillsynsmyndigheten för dataskyddsförordningen när de behandlar incidenter som medför personuppgiftsincidenter.

Tillsyn och efterlevnadskontroller av väsentliga verksamhetsutövare

Enligt artikel 32.1 ska medlemsstaterna säkerställa att de tillsyns- eller efterlevnadskontroller som åläggs väsentliga verksamhetsutövare är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall. Enligt artikel 32.2 ska medlemsstaterna säkerställa att den behöriga myndigheten, när den utövar sina tillsynsuppgifter, har befogenhet att åtminstone underställa dessa verksamhetsutövare:

- a) inspektioner på plats och distansbaserad tillsyn,
- b) regelbundna och riktade säkerhetsrevisioner,
- c) ad hoc-revisioner,
- d) säkerhetsskanningar,
- e) begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av verksamhetsutövaren,
- f) begäranden om tillgång till uppgifter, handlingar och information som behövs för att de ska kunna utföra sina tillsynsuppgifter, och
- g) begäranden om bevis på genomförandet av cybersäkerhetsstrategier.

Kostnaderna för riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av verksamhetsutövaren, om inte den behöriga myndigheten beslutar något annat.

Enligt artikel 32.4 ska medlemsstaterna vidare säkerställa att behöriga myndigheter, när de utövar efterlevnadskontroll, åtminstone har befogenhet att:

- a) utfärda varningar,
- b) anta bindande instruktioner,
- c) ålägga de berörda verksamhetsutövarna att upphöra med och att avstå från att upprepa beteenden som utgör en överträdelse av direktivet,
- d) ålägga de berörda verksamhetsutövarna att säkerställa riskhanteringsåtgärder och incidentrapportering överensstämmer med direktivet,
- e) ålägga de berörda verksamhetsutövarna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför verksamheter som potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpanande åtgärder som dessa kan vidta som svar på hotet,
- f) ålägga de berörda verksamhetsutövarna att genomföra rekommendationer som lämnats till följd av en säkerhetsrevision,
- g) utse en övervakningsansvarig för att övervaka att verksamhetsutövaren efterlever skyldigheter om riskhanteringsåtgärder och incidentrapportering,
- h) ålägga de berörda verksamhetsutövarna att offentliggöra aspekter av överträdelser av direktivet, och
- i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter.

Enligt artikel 32.5 ska medlemsstaterna, om efterlevnadskontrollåtgärderna är ineffektiva, säkerställa att den behöriga myndigheten har befogenhet att fastställa en tidsfrist inom vilken en väsentlig verksamhetsutövare ska vidta nödvändiga åtgärder för att avhjälpa bristerna. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att den behöriga myndigheten har befogenhet att:

- a) 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 verksamhetsutövaren, och
- b) begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån verkställande direktör eller juridiskt ombud har ledningsansvar i verksamhetsutövaren att utöva ledningsfunktioner.

Tillfälliga upphävanden och förbud är inte tillämpliga på offentliga verksamhetsutövare som omfattas av direktivet.

Enligt artikel 32.6 ska medlemsstaterna säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en verksamhetsutövare har befogenhet att säkerställa att verksamhetsutövaren efterlever direktivet. Medlemsstaterna ska också säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att direktivet efterlevs. När det gäller offentliga verksamhetsutövare påverkar detta inte nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

Enligt artikel 32.9 ska medlemsstaterna säkerställa att deras behöriga myndigheter informerar relevanta behöriga myndigheter enligt motståndskraftsdirektivet när de utövar sina befogenheter med avseende på tillsyn och

efterlevnads kontroll mot en verksamhetsutövare som identifierats som en kritisk verksamhetsutövare enligt det direktivet.

Tillsyn och efterlevnads kontroller av viktiga verksamhetsutövare

Enligt artikel 33.1 ska medlemsstaterna, när de får bevis, indikationer på eller information, om att en viktig verksamhetsutövare påstås underlåta att fullgöra direktivet, säkerställa att den behöriga myndigheten vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

Enligt artikel 33.2 ska medlemsstaterna säkerställa att den behöriga myndigheten, när den utövar sina tillsynsuppgifter avseende viktiga verksamhetsutövare, har i princip samma befogenheter som de har gällande väsentliga verksamhetsutövare, med skillnaden att tillsyn ska ske i efterhand.

Enligt artikel 33.4 ska medlemsstaterna också säkerställa att den behöriga myndigheten har i stora delar samma befogenheter när det gäller efterlevnads kontroll som den har gällande väsentliga verksamhetsutövare. Dock återfinns inte bestämmelsen om den för väsentliga verksamhetsutövare motsvarande möjligheten att utse en övervakningsansvarig när det gäller viktiga verksamhetsutövare, eller om att upphäva certifiering eller auktorisation eller införa förbud för personer att utöva ledningsansvar.

2.2.16 Sanktioner

Enligt artikel 34.1 ska medlemsstaterna fastställa regler om administrativa sanktionsavgifter för överträdelse av det nationella genomförandet, vilka ska vara effektiva proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

Enligt artikel 34.4 ska medlemsstaterna säkerställa att väsentliga verksamhetsutövare som överträder artikel 21 eller 23 påförs administrativa sanktionsavgifter på högst 10 000 000 euro eller högst 2 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

Enligt artikel 34.5 ska medlemsstaterna säkerställa att viktiga verksamhetsutövare som överträder artikel 21 eller 23 påförs administrativa sanktionsavgifter på högst 7 000 000 euro eller högst 1,4 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst.

Enligt artikel 34.6 får medlemsstaterna föreskriva befogenhet att förelägga viten för att tvinga en verksamhetsutövare att upphöra med en överträdelse av direktivet.

Enligt artikel 34.7 får medlemsstaterna också fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga verksamhetsutövare.

2.3 Direktivet om kritisk infrastruktur

2.3.1 Bakgrund och syfte

Den 8 december 2008 antogs Rådets direktiv (EG) 2008/114 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömningen av behovet att stärka skyddet av denna (nedan kallat *direktivet om kritisk infrastruktur*).

Syftet med direktivet om kritisk infrastruktur var att fastställa ett förfarande för identifiering av, och klassificering som, europeisk kritisk

infrastruktur och en gemensam metod för bedömning av behovet att stärka skyddet av sådan infrastruktur för att bidra till att skydda människor.

I direktivet föreskrivs ett förfarande för att klassificera infrastruktur i energi- och transportsektorerna som europeisk kritisk infrastruktur, vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Direktivet var uteslutande inriktat på skyddet av sådan infrastruktur och vid den utvärdering som gjordes 2019 konstaterades dock att skyddsåtgärder som enbart gäller enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå, på grund av den alltmer sammankopplade och gränsöverskridande karaktären hos den verksamhet vilken bedrivs med kritisk infrastruktur.

2.3.2 Genomförandet på Åland

Landskapsregeringen bedömde vid tiden för direktivet om kritisk infrastruktur genomförande att frågan föll inom ramen för rikets lagstiftningsbehörighet över beredskapen inför undantagsförhållanden, enligt 27 § 34 punkten självstyrelselagen, och landskapets behörighet, enligt 18 § 21 punkten gällande vägar, kanaler, vägtrafik, spårbunden trafik, båttrafik samt farleder för den lokala sjötrafiken. I dag gör Ålands landskapsregering en annan bedömning, se närmare redogörelse av lagstiftningsbehörigheten avseende motståndskraftdirektivet under avsnitt 4 nedan. Oavsett genomfördes aldrig direktivet om kritisk infrastruktur på Åland. De berörda verksamhetsutövarna har hittills, i varierande grad och till följd av rikets lagstiftningsbehörighet över verksamhetsområdet eller blankettlagstiftning, tillämpat rikets reglering i den sektorsspecifika speciallagstiftningen.

2.3.3 Genomförandet i riket

Direktiv (EG) 2008/114 genomfördes i huvudsak i riket genom lagändringar i förevarande sektorspecifik lagstiftning. Det stiftades därmed inte någon nationell, horisontell allmän lag, vari direktivets bestämmelser genomfördes, utan det genomfördes genom att skyldigheterna införlivades i den talrika sektorspecifika speciallagstiftningen. Tillsynen över av att skyldigheterna enligt genomförandet efterföljdes utfördelades därmed på flera olika sektorspecifika myndigheter.

2.4 Motståndskraftdirektivet (CER-direktivet)

2.4.1 Bakgrund och syfte

Den 14 december 2022 antog Europaparlamentet och rådet motståndskraftdirektivet. Enligt artikel 1.1 är motståndskraftdirektivets syfte att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet tillhandahålls på ett obehindrat sätt på den inre marknaden, att stärka kritiska verksamhetsutövarers motståndskraft och att uppnå en hög grad av motståndskraft för kritiska verksamhetsutövare, för att säkerställa tillhandahållande av samhällsviktiga tjänster i unionen och förbättra den inre marknads funktionssätt.

Enligt artikel 3 utgör motståndskraftdirektivet ett minimidirektiv, med innebörden att den åländska lagstiftningen skulle kunna innehålla mer långtgående skyldigheter.

Enligt skäl 1 spelar kritiska verksamhetsutövare, som tillhandahållare av samhällsviktiga tjänster, en oumbärlig roll när det gäller att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden, i en unionsekonomi som i allt högre grad kännetecknas av ömsesidigt beroende. Det är därför mycket viktigt att det inrättas en unionsram som syftar dels till att stärka kritiska verksamhetsutövarers motståndskraft på den inre marknaden, genom att fastställa harmoniserade minimiregler, dels

till att bistå verksamhetsutövarna genom enhetligt och särskilt stöd och tillsynsåtgärder.

Enligt skäl 2 är de skyddsåtgärder som enbart gäller enskilda tillgångar inom infrastruktur inte tillräckliga för att förhindra alla störningar från att uppstå, på grund av den alltmer sammankopplade och gränsöverskridande karaktären hos den verksamhet som bedrivs med kritisk infrastruktur. Därför är det nödvändigt att ändra ansatsen i riktning mot att säkerställa att risker redovisas bättre, att bättre definiera och skapa enhetlighet i rollen och uppgifterna för kritiska verksamhetsutövare i egenskap av tillhandahållare av tjänster som är nödvändiga för att den inre marknaden ska kunna fungera, och att unionsregler antas för att stärka kritiska verksamhetsutövares motståndskraft. Kritiska verksamhetsutövare bör kunna öka sin förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från incidenter som kan störa tillhandahållandet av samhällsviktiga tjänster.

Enligt skäl 3 bör, samtidigt som ett antal åtgärder på unionsnivå, såsom det europeiska programmet för skydd av kritisk infrastruktur, och nationell nivå syftar till att stödja skyddet av kritisk infrastruktur i unionen, mer göras för att de verksamhetsutövare som driver sådan infrastruktur ska vara bättre rustade att hantera de risker för deras verksamhet som kan leda till störningar i tillhandahållandet av samhällsviktiga tjänster. Mer bör också göras för att bättre rusta sådana verksamhetsutövare eftersom det finns en dynamisk hotbild, som inbegriper framväxande hybrid- och terroristhot, och ett ökande ömsesidigt beroende mellan infrastruktur och sektorer. Dessutom finns det en ökad fysisk risk på grund av naturkatastrofer och klimatförändringen, som leder till att extrema väderhändelser blir allt vanligare och mer omfattande och medför långsiktiga förändringar i genomsnittliga klimatförhållanden som kan minska kapaciteten, effektiviteten och livslängden för vissa typer av infrastruktur om det inte vidtas klimatanpassningsåtgärder. Den inre marknaden kännetecknas dessutom av fragmentering när det gäller identifiering av kritiska verksamhetsutövare, eftersom relevanta sektorer och kategorier av verksamhetsutövare inte erkänns på ett enhetligt sätt som kritiska i alla medlemsstater. Direktivet bör därför åstadkomma en solid harmoniseringsnivå när det gäller de sektorer och kategorier av verksamhetsutövare som omfattas av dess tillämpningsområde.

Enligt skäl 4 är vissa sektorer inom ekonomin, exempelvis energi- och transportsektorerna, redan reglerade genom sektorsspecifika unionsrättsakter, men dessa rättsakter innehåller bestämmelser som endast rör vissa aspekter av motståndskraften hos verksamhetsutövare som är verksamma inom de sektorerna. För att på ett heltäckande sätt hantera motståndskraften hos de verksamhetsutövare som är kritiska för att den inre marknaden ska fungera väl inrättas genom direktivet en övergripande ram för att hantera kritiska verksamhetsutövares motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller faror orsakade av människan, olycks-händelser eller avsiktligt framkallade faror.

Enligt skäl 5 är det ökande ömsesidiga beroendet mellan infrastruktur och sektorer ett resultat av ett alltmer gränsöverskridande och ömsesidigt beroende nätverk av tillhandahållande av tjänster som använder viktig infrastruktur i hela unionen inom sektorerna för energi, transporter, bankverksamhet, dricksvatten, avloppsvatten, produktion, bearbetning och distribution av livsmedel, hälso- och sjukvård, rymden, finansmarknadsinfrastruktur och digital infrastruktur samt vissa aspekter av sektorn för offentlig förvaltning. Detta ömsesidiga beroende innebär att alla störningar av samhällsviktiga tjänster, även sådana som till en början är begränsade till en verksamhetsutövare eller en sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga negativa konsekvenser för tillhandahållandet av tjänster på hela den inre marknaden. Större kriser såsom covid-19-pandemin

har visat hur sårbara våra alltmer av varandra beroende samhällen är för risker med låg sannolikhet och stora konsekvenser.

Enligt skäl 6 omfattas de verksamhetsutövare som deltar i tillhandahållandet av samhällsviktiga tjänster i allt högre grad av olika krav som införs enligt nationell rätt. Vissa medlemsstater ställer mindre hårda säkerhetskrav på dessa verksamhetsutövare, vilket inte bara leder till olika grad av motståndskraft utan också riskerar att ge negativa effekter för upprätthållandet av viktiga samhällsfunktioner eller central ekonomisk verksamhet i unionen och skapar hinder för den inre marknadens funktion. Investerare och företag kan förlita sig på och ha förtroende för kritiska verksamhetsutövare som är motståndskraftiga, och tillförlitlighet och förtroende är hörnstenar i en välfungerande inre marknad. Likartade typer av verksamhetsutövare betraktas som kritiska i vissa medlemsstater men inte i andra, och de som identifieras som kritiska omfattas av olika krav i olika medlemsstater. Detta leder till en ytterligare och onödigt administrativ börda för företag som bedriver gränsöverskridande verksamhet, särskilt för företag med verksamhet i medlemsstater som ställer hårdare krav. En unionsram skulle därför också leda till likvärdiga förutsättningar för kritiska verksamhetsutövare i hela unionen.

Enligt skäl 7 är det nödvändigt att införa harmoniserade minimiregler för att säkerställa tillhandahållandet av samhällsviktiga tjänster på den inre marknaden, stärka kritiska verksamhetsutövares motståndskraft samt förbättra det gränsöverskridande samarbetet mellan behöriga myndigheter. Det är viktigt att dessa regler är framtidssäkrade när det gäller utformning och genomförande, samtidigt som utrymme ges för den flexibilitet som krävs. Det är också mycket viktigt att förbättra kritiska verksamhetsutövares förmåga att tillhandahålla samhällsviktiga tjänster med avseende på en rad olika risker.

2.4.2 Innehåll och tillämpningsområde

Enligt artikel 1.1 innehåller direktivet skyldigheter för medlemsstaterna och identifierade kritiska verksamhetsutövare samt åtgärder som dessa ska vidta för att öka kritiska verksamhetsutövares motståndskraft. Enligt artikel 2.1 definieras kritiska verksamhetsutövare som en offentlig eller privat verksamhetsutövare som har identifieras av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan. I artikel 2.2 definieras motståndskraft som en kritisk verksamhetsutövares förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident.

Enligt bilagan kan kategorier av verksamhetsutövare inom följande sektorer och undersektorer anses kritiska:

1. Energi, med undersektorerna:
 - a) elektricitet,
 - b) fjärrvärme eller fjärrkyla,
 - c) olja,
 - d) gas, och
 - e) vätgas.
2. Transport, med undersektorerna:
 - a) luftfart,
 - b) järnväg,
 - c) vatten,
 - d) väg, och
 - e) kollektivtrafik.
3. Bankverksamhet
4. Finansmarknadsinfrastruktur
5. Hälso- och sjukvård
6. Dricksvatten

7. Avloppsvatten
8. Digital infrastruktur
9. Offentlig förvaltning
10. Rymden
11. Produktion, bearbetning och distribution av livsmedel

Enligt artikel 1.2 ska direktivet inte vara tillämpligt på frågor som omfattas av cybersäkerhetsdirektivet och, med beaktande av förhållandet mellan kritiska verksamhetsutövers fysiska säkerhet och cybersäkerhet, ska medlemsstaterna säkerställa att direktiven genomförs på ett samordnat sätt.

Enligt artikel 1.3 ska berörda bestämmelser i direktivet, om det enligt bestämmelser i sektorsspecifika unionsrättsakter krävs att kritiska verksamhetsutövare ska vidta åtgärder för att stärka sin motståndskraft och om de kraven erkänns av medlemsstaterna som åtminstone likvärdiga med de motsvarande skyldigheter som fastställs i direktivet, inte vara tillämpligt.

Enligt artikel 1.4 ska information som är konfidentiell enligt unionsregler eller nationella regler, såsom regler om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter i enlighet med direktivet endast när sådant utbyte är nödvändigt för att tillämpa detta. Den information som utbyts ska begränsas till vad som är relevant och proportionerligt för ändamålet med utbytet. Vid informationsutbytet ska informationens konfidentialitet och kritiska verksamhetsutövers säkerhetsintressen och kommersiella intressen bevaras samtidigt som medlemsstaternas säkerhet respekteras.

Enligt artikel 1.5 påverkar direktivet inte medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

Enligt artikel 1.6 är direktivet inte tillämpligt på offentliga verksamhetsutövare som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Enligt artikel 1.7 får medlemsstaterna besluta att artikel 11 och kapitlen III, IV och VI, helt eller delvis, inte är tillämpliga på särskilda kritiska verksamhetsutövare som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott, eller som uteslutande tillhandahåller tjänster till offentliga verksamhetsutövare. Enligt artikel 1.8 får de skyldigheter som fastställs i direktivet inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

Enligt artikel 1.9 påverkar direktivet inte tillämpningen av andra unionsrättsakter om skydd av personuppgifter.

Samhällsviktiga tjänster och förteckning

I artikel 2.5 definieras samhällsviktig tjänst som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. I enlighet med artikel 5 antog kommissionen den 25 juli 2023 en delegerad förordning, (EU) 2023/2450 om komplettering av motståndskraftsdirektivet genom upprättande av en förteckning över samhällsviktiga tjänster, vilken utgör en icke uttömmande förteckning över samhällsviktiga tjänster som kategorierna av verksamhetsutövare inom respektive undersektor i bilagan kan tillhandahålla. Enligt förordningen utgör följande tjänster samhällsviktiga tjänster:

1. Energisektorn:
 - a. Undersektorn elektricitet:
 - i. Leverans av el (*elföretag*).

- ii. Drift, underhåll och utveckling av ett eldistributionssystem (*systemansvariga för distributionssystemet*).
 - iii. Drift, underhåll och utveckling av ett elöverföringssystem (*systemansvariga för överföringssystemet*).
 - iv. Elproduktion (*producenter*).
 - v. Nominerade elmarknadsoperatörers tjänster (*nominerade elmarknadsoperatörer*).
 - vi. Efterfrågeflexibilitet (*elmarknadsaktörer*).
 - vii. Aggregering av el (*elmarknadsaktörer*).
 - viii. Energilagring (*elmarknadsaktörer*).
- b. Undersektorn fjärrvärme och fjärrkyla: Tillhandahållande av fjärrvärme eller fjärrkyla (*operatörer av fjärrvärme eller fjärrkyla*).
- c. Undersektorn olja:
- i. Överföring av olja (*operatörer av oljeledningar*).
 - ii. Oljeproduktion (*operatörer av anläggningar för oljeproduktion*).
 - iii. Raffinering och bearbetning av olja (*operatörer av raffinaderier och bearbetningsanläggningar för olja*).
 - iv. Lagring av olja (*operatörer av anläggningar för lagring av olja*).
 - v. Förvaltning av oljelager, inklusive beredskapslager och särskilda oljelager (*centrala lagringsenheter*).
- d. Undersektorn gas:
- i. Gasleverans eller gashandel (*gashandelsföretag eller gashandlare*).
 - ii. Distribution av gas (*systemansvariga för distributionssystemet*).
 - iii. Överföring av gas (*systemansvariga för överföringssystemet*).
 - iv. Lagring av gas (*systemansvariga för lagringssystemet*).
 - v. Drift av ett system för flytande naturgas (LNG) (*systemansvariga för en LNG-anläggning*).
 - vi. Produktion av naturgas (*naturgasföretag*).
 - vii. Inköp av naturgas (*naturgasföretag*).
 - viii. Raffinering och bearbetning av naturgas (*operatörer av raffinaderier och bearbetningsanläggningar för naturgas*).
- e. Undersektorn vätgas:
- i. Produktion av vätgas (*operatörer av produktion av vätgas*).
 - ii. Lagring av vätgas (*operatörer av lagring av vätgas*).
 - iii. Överföring av vätgas (*operatörer av överföring av vätgas*).
2. Transportsektorn:
- a. Undersektorn luftfart:
- i. Lufttransporttjänster som används för kommersiella syften (passagerare och frakt) (*lufttrafikföretag*).
 - ii. Drift, förvaltning och underhåll av flygplatser och av flygplatsnätets infrastruktur (*flygplatsernas ledningsenheter*).
 - iii. Flygkontrolltjänster (*operatörer inom trafikstyrning och trafikledning*).

- b. Undersektorn järnväg:
 - i. Järnvägstransporttjänster (passagerare och frakt) (*järnvägsföretag*).
 - ii. Drift, förvaltning och underhåll av järnvägsinfrastruktur, inbegripet stationer för passagerare, gods-terminaler, bangårdar och trafikledningscentraler (*infrastrukturförvaltare*).
 - iii. Drift, förvaltning och underhåll av anläggningar för järnvägstjänster (*tjänsteleverantörer*).
 - iv. Drift, förvaltning och underhåll av trafikledning, trafikstyrning och signalering samt installationer och system för telekommunikation som används för trafikstyrning och signalering (*infrastrukturförvaltare*).
- c. Undersektorn vatten:
 - i. Transporttjänster på inre vattenvägar, till havs och längs kuster (passagerar- och godstrafik) (*passagerar- och godstransportföretag på inre vattenvägar, till havs och längs kuster*).
 - ii. Drift, ledning och underhåll av hamnar och hamnanläggningar samt drift av anläggningar och utrustning i hamnar, inbegripet bunkring, lasthantering, förtöjning, passagerartjänster, insamling av fartygs-genererat avfall och lastrester, lotsning och bogsering (*ledningsenheter för hamnar och verksamhetsutövare som sköter anläggningar och utrustning i hamnar*).
 - iii. Sjötrafikinformationstjänst (*operatörer av sjötrafikinformationstjänst*).
- d. Undersektorn vägtransport:
 - i. Trafikstyrning, inbegripet aspekter som rör planering, kontroll och förvaltning av vägnät, med undantag för trafikstyrning eller drift av intelligenta transportsystem när dessa inte utgör en väsentlig del av den allmänna verksamheten för offentliga verksamhetsutövare (*vägmyndigheter*).
 - ii. Intelligenta transportsystem (*operatörer av intelligenta transportsystem*).
- e. Undersektorn kollektivtrafik: Kollektivtrafik på järnväg samt med andra spårbaserade transportsätt och på väg (*kollektivtrafikföretag*).
- 3. Banksektorn:
 - a. Mottagande av insättningar (*kreditinstitut*).
 - b. Utlåning (*kreditinstitut*).
- 4. Sektorn finansmarknadsinfrastruktur:
 - a. Drift av en handelsplats (*operatörer av handelsplatser*).
 - b. Drift av clearingsystem (*centrala motparter*).
- 5. Hälso- och sjukvårdssektorn:
 - a. Tillhandahållande av hälso- och sjukvårdstjänster (*vårdgivare*).
 - b. Analys som utförs av ett av Europeiska unionens referenslaboratorier (*EU:s referenslaboratorier*).
 - c. Forskning om och utveckling avseende läkemedel (*verksamhetsutövare som bedriver forskning om och utveckling avseende läkemedel*).

- d. Tillverkning av farmaceutiska basprodukter och basläkemedel (*verksamhetsutövare som tillverkar farmaceutiska basprodukter och läkemedel*).
 - e. Tillverkning av medicintekniska produkter som betraktas som kritiska vid ett hot mot folkhälsan (*verksamhetsutövare som tillverkar medicintekniska produkter*).
 - f. Distribution av läkemedel (*verksamhetsutövare med tillstånd att bedriva partihandel*).
6. Dricksvattensektorn: Dricksvattenförsörjning och distribution av dricksvatten, med undantag för distribution av dricksvatten när denna tjänst utgör en icke väsentlig del av den allmänna verksamheten för distributörer som distribuerar andra förnödenheter och varor (*leverantörer och distributörer av dricksvatten*).
 7. Avloppsvattensektorn: Insamling, rening och utsläpp av avloppsvatten, med undantag för insamling, utsläpp eller rening av avloppsvatten från tätbebyggelse, hushållspillvatten eller industrispillvatten när detta inte utgör en väsentlig del av företagets allmänna verksamhet (*verksamheter som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållspillvatten eller industrispillvatten*).
 8. Sektorn digital infrastruktur:
 - a. Tillhandahållande och drift av internetknutpunkter (*leverantörer av internetknutpunkter*).
 - b. Tillhandahållande av domännamnssystem (DNS) med undantag för tjänster som rör rotnamnservrar (*leverantörer av DNS-tjänster*).
 - c. Drift och administration av registreringsenheter för toppdomäner (*registreringsenheter för toppdomäner*).
 - d. Tillhandahållande av molntjänster (*leverantörer av molntjänster*).
 - e. Tillhandahållande av datacentralstjänster (*tillhandahållare av datacentralstjänster*).
 - f. Tillhandahållande av nätverk för innehållsleverans (*tillhandahållare av nätverk för innehållsleverans*).
 - g. Tillhandahållande av betrodda tjänster (*tillhandahållare av betrodda tjänster*).
 - h. Tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster (*tillhandahållare av elektroniska kommunikationstjänster*).
 - i. Tillhandahållande av allmänna elektroniska kommunikationsnät (*tillhandahållare av allmänna elektroniska kommunikationsnät*).
 9. Sektorn offentlig förvaltning: Tjänster som tillhandahålls av offentliga verksamhetsutövare i den mening som avses i artikel 2.10 i direktiv (EU) 2022/2557 hos nationella regeringar enligt medlemsstaternas definition i enlighet med nationell rätt (*offentliga verksamhetsutövare hos nationella regeringar*).
 10. Rymdsektorn: Drift av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät (*operatörer av markbaserad infrastruktur*).
 11. Produktion, bearbetning och distribution av livsmedel (*livsmedelsföretag som uteslutande bedriver logistikverksamhet och grossisthandel samt storskalig industriell produktion och bearbetning*):
 - a. Storskalig industriell produktion och bearbetning av livsmedel.

- b. Tjänster inom livsmedelskedjan, inbegripet lagring och logistik.
- c. Grossisthandel med livsmedel.

2.4.3 Behörig myndighet och gemensam kontaktpunkt

Enligt artikel 9.1 ska varje medlemsstat utse eller inrätta en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, vid behov, efterlevnadskontrollen avseende reglerna i direktivet på nationell nivå. När det gäller kritiska verksamhetsutövare enligt punkterna 3 och 4 i bilagans tabell ska behöriga myndigheter i princip vara de som avses i artikel 46 i Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (nedan kallad *motståndskraftsförordningen för finanssektorn*, även kallad DORA-förordningen efter engelskans *Digital Operative Resilience Act*). När det gäller kritiska verksamhetsutövare enligt punkten 8 i bilagans tabell ska de behöriga myndigheterna i princip vara de behöriga myndigheterna enligt cybersäkerhetsdirektivet. Medlemsstaterna får utse en annan behörig myndighet för de sektorer som anges i punkterna 3, 4 och 8 i bilagans tabell för motståndskraftsdirektivet i enlighet med befintliga nationella ramar. Om medlemsstaterna utser eller inrättar mer än en behörig myndighet ska de tydligt fastställa uppgifterna för var och en av de berörda myndigheterna och säkerställa att de samarbetar effektivt för att fullgöra sina uppgifter enligt direktivet.

Enligt artikel 9.2 ska varje medlemsstat utse eller inrätta en gemensam kontaktpunkt, vilken ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med de gemensamma kontaktpunkterna i andra medlemsstater och den grupp för kritiska verksamheters motståndskraft som avses i artikel 19. I förekommande fall ska en medlemsstat utse sin gemensamma kontaktpunkt inom en behörig myndighet och får därutöver föreskriva att dess gemensamma kontaktpunkt även ska ha en sambandsfunktion med kommissionen och säkerställa samarbete med tredjeländer.

2.4.4 Nationellt samarbete

Enligt artikel 9.6 ska varje medlemsstat säkerställa att den behöriga myndigheten samarbetar och utbyter information med de behöriga myndigheterna enligt cybersäkerhetsdirektivet om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska verksamhetsutövare, inbegripet avseende relevanta åtgärder som har vidtagits av behöriga myndigheter.

Enligt artikel 10.2 ska varje medlemsstat säkerställa att den behöriga myndigheten samarbetar och utbyter information och god praxis med kritiska verksamhetsutövare i de sektorer som anges i bilagan.

Enligt artikel 10.3 ska medlemsstaterna underlätta frivillig informationsdelning mellan kritiska verksamhetsutövare i frågor som omfattas av direktivet, i enlighet med unionsrätten och nationell rätt, särskilt i fråga om sekretessbelagd och känslig information, konkurrens och skydd av personuppgifter.

Enligt artikel 21.5 ska medlemsstaterna säkerställa att när en behörig myndighet enligt motståndskraftsdirektivet bedömer efterlevnaden hos en kritisk verksamhetsutövare enligt artikel 21 ska den behöriga myndigheten informera de behöriga myndigheterna i de berörda medlemsstaterna enligt cybersäkerhetsdirektivet. I detta syfte ska medlemsstaterna säkerställa att de behöriga myndigheterna enligt det här direktivet kan begära att de behöriga myndigheterna enligt direktiv cybersäkerhetsdirektivet ska utöva sina tillsyns- och efterlevnadskontrollbefogenheter med avseende på en verksamhetsutövare enligt det direktivet som har identifierats som en kritisk verksamhetsutövare enligt motståndskraftsdirektivet. För det ändamålet ska

medlemsstaterna säkerställa att de behöriga myndigheterna enligt det här direktivet samarbetar och utbyter information med de behöriga myndigheterna enligt direktiv cybersäkerhetsdirektivet.

2.4.5 Samarbete mellan medlemsstater

Enligt artikel 11 ska medlemsstaterna, när så är lämpligt, samråda med varandra om kritiska verksamhetsutövare i syfte att säkerställa att direktivet tillämpas på ett konsekvent sätt. Sådana samråd ska äga rum i synnerhet med avseende på kritiska verksamhetsutövare som:

- a) använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller flera medlemsstater,
- b) ingår i företagsstrukturer som är sammankopplade eller sammanlänkade med kritiska verksamhetsutövare i andra medlemsstater,
- c) har identifierats som kritiska verksamhetsutövare i en medlemsstat och tillhandahåller samhällsviktiga tjänster för eller i andra medlemsstater.

Enligt artikel 11.2 ska samråden syfta till att stärka kritiska verksamhetsutövare motståndskraft och, om möjligt, minska deras administrativa börda.

2.4.6 Gruppen för kritiska entiteters motståndskraft

Enligt artikel 19.1 inrättas en grupp för kritiska entiteters motståndskraft, vilken ska ge kommissionen stöd och underlätta samarbete mellan medlemsstaterna och informationsutbyte om frågor som rör direktivet. Enligt artikel 19.2 ska gruppen bestå av företrädare för medlemsstaterna och kommissionen, vid behov med säkerhetsgodkännande. Gruppen för kritiska entiteters motståndskraft får bjuda in andra berörda parter att delta i sitt arbete när detta är relevant för fullgörandet av gruppens uppgifter. Om Europaparlamentet så begär får kommissionen bjuda in experter från Europaparlamentet att närvara vid möten i gruppen för kritiska entiteters motståndskraft.

Enligt artikel 19.3 tilldelas gruppen särskilda uppgifter enligt artikel 19.3 och ska enligt artikel 19.4 utarbeta ett arbetsprogram senast den 17 januari 2025, samt därefter vartannat år, och enligt artikel 19.5 sammanträda minst årligen med samarbetsgruppen enligt cybersäkerhetsdirektivet.

2.4.7 Medlemsstaternas riskbedömning

Enligt artikel 5.1 ges kommissionen befogenhet att anta en delegerad akt i enlighet med artikel 23 senast den 17 november 2023 för att komplettera direktivet genom att upprätta en icke uttömmande förteckning över samhällsviktiga tjänster inom de sektorer och undersektorer som anges i bilagan.

De behöriga myndigheterna ska använda kommissionens förteckning över samhällsviktiga tjänster för att göra en riskbedömning, den så kallade medlemsstaternas riskbedömning, senast den 17 januari 2026 och därefter när så är nödvändigt och minst vart fjärde år. De behöriga myndigheterna ska använda medlemsstaternas riskbedömningar i syfte att identifiera kritiska verksamhetsutövare i enlighet med och bistå de kritiska verksamhetsutövarna med att vidta åtgärder.

Medlemsstaternas riskbedömningar ska innehålla en redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot, inklusive terroristbrott enligt Europaparlamentets och rådets direktiv (EU) 2017/541 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF.

Enligt artikel 5.2 ska medlemsstaternas riskbedömningar åtminstone ta hänsyn till följande:

- a) Den allmänna riskbedömning som har utförts enligt artikel 6.1 i beslut nr 1313/2013/EU.
- b) Andra relevanta riskbedömningar som har utförts i enlighet med kraven i relevanta sektorsspecifika unionsrättsakter, inbegripet Europaparlamentets och rådets förordningar (EU) 2017/1938 och (EU) 2019/941 och Europaparlamentets och rådets direktiv 2007/60/EG och 2012/18/EU.
- c) De relevanta risker som uppstår till följd av den grad till vilken de sektorer som anges i bilagan är beroende av varandra, inbegripet den grad till vilken de är beroende av verksamhetsutövare som är belägna i andra medlemsstater och tredjeländer, samt de konsekvenser en betydande störning i en sektor kan få för andra sektorer, inklusive eventuella betydande risker för medborgare och den inre marknaden.
- d) Information om incidenter som har anmälts i enlighet med artikel 15.

Vid tillämpning av artikel 5.2 punkten c ska medlemsstaterna samarbeta med de behöriga myndigheterna i andra medlemsstater och de behöriga myndigheterna i tredjeländer, när så är lämpligt.

Enligt artikel 5.3 ska medlemsstaterna, i förekommande fall genom sina gemensamma kontaktpunkter, göra de relevanta delarna i deras riskbedömningar tillgängliga för de kritiska verksamhetsutövare som de har identifierat och säkerställa att den information som tillhandahålls hjälper dem att utföra sina egna riskbedömningar och vidtagande av åtgärder för att säkerställa sin motståndskraft.

2.4.8 Medlemsstaternas identifiering av kritiska verksamhetsutövare

Enligt artikel 6.1 ska medlemsstaterna, senast den 17 juli 2026 identifiera de kritiska verksamhetsutövarna för de sektorer och undersektorer som anges i bilagan.

Enligt artikel 6.2 ska en medlemsstat, när den identifierar kritiska verksamhetsutövare ta hänsyn till resultatet av sin riskbedömning samt sin strategi och tillämpa samtliga följande kriterier:

- a) Verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster.
- b) Verksamhetsutövaren bedriver verksamhet, och dess kritiska infrastruktur är belägen, på denna medlemsstats territorium.
- c) En incident skulle få betydande störande effekter, enligt vad som fastställs i enlighet med artikel 7.1, för verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra samhällsviktiga tjänster i de sektorer som anges i bilagan och som är beroende av den eller de samhällsviktiga tjänsterna.

Enligt artikel 6.3 ska varje medlemsstat upprätta en förteckning över de kritiska verksamhetsutövare som har identifierats enligt artikel 6.2 och säkerställa att dessa kritiska verksamhetsutövare underrättas om att de har identifierats som kritiska verksamhetsutövare inom en månad från identifieringen. Medlemsstaterna ska informera dessa kritiska verksamhetsutövare om deras skyldigheter enligt kapitlen III och IV och om det datum från och med vilket dessa skyldigheter är tillämpliga på dem, utan att detta påverkar tillämpningen av artikel 8. Medlemsstaterna ska informera kritiska verksamhetsutövare i de sektorer som anges i punkterna 3, 4 och 8 i bilagans tabell om att de inte har några skyldigheter enligt kapitlen III och IV såvida inte nationella åtgärder föreskriver något annat. För de berörda kritiska verksamhetsutövarna ska kapitel III vara tillämpligt från och med tio månader efter dagen för underrättelsen.

Enligt artikel 6.4 ska medlemsstaterna säkerställa att deras behöriga myndigheter underrättar de behöriga myndigheterna enligt

cybersäkerhetsdirektivet om identitet på de kritiska verksamhetsutövare som de har identifierat inom en månad från den identifieringen. Denna underrättelse ska, i tillämpliga fall, innehålla information om att de berörda kritiska verksamhetsutövarna är verksamhetsutövare i de sektorer som anges i punkterna 3, 4 och 8 i bilagans tabell och inte har några skyldigheter enligt kapitlet III och IV i direktivet.

Enligt artikel 6.5 ska medlemsstaterna, när så är nödvändigt och minst vart fjärde år, se över och när så är lämpligt uppdatera förteckningen över identifierade kritiska verksamhetsutövare som avses i artikel 6.3. Om dessa uppdateringar leder till att ytterligare kritiska verksamhetsutövare identifieras ska artikel 6.3–4 tillämpas på dessa. Dessutom ska medlemsstaterna säkerställa att verksamhetsutövare som inte längre identifieras som kritiska verksamhetsutövare till följd av en sådan uppdatering i god tid underrättas om detta och om att de inte längre omfattas av skyldigheterna enligt kapitel III från och med dagen för mottagandet av denna underrättelse.

Medlemsstaternas identifiering av kritiska verksamhetsutövare av särskild europeisk betydelse

Enligt artikel 17.1 ska en verksamhetsutövare betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse om:

- a) den har identifierats som en kritisk verksamhetsutövare enligt artikel 6.1,
- b) den tillhandahåller samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater, och
- c) den har mottagit en underrättelse av kommissionen enligt artikel 17.3.

Enligt artikel 17.2 ska medlemsstaterna säkerställa att en kritisk verksamhetsutövare, efter den underrättelse som avses i artikel 6.3, informerar sin behöriga myndighet om den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater. I ett sådant fall ska medlemsstaterna säkerställa att den kritiska verksamhetsutövaren underrättar sin behöriga myndighet om de samhällsviktiga tjänster som den tillhandahåller till eller i dessa medlemsstater och till eller i vilka medlemsstater den tillhandahåller sådana samhällsviktiga tjänster. Medlemsstaterna ska utan onödigt dröjsmål underrätta kommissionen om identiteten på dessa kritiska verksamhetsutövare och den information som de tillhandahåller enligt denna punkt.

Enligt artikel 17.4 ska bestämmelserna om kritiska verksamhetsutövare av särskild europeisk betydelse tillämpas på relevanta verksamhetsutövare från och med dagen för mottagandet av den underrättelse som avses i artikel 17.3.

2.4.9 Betydande störande effekt

Enligt artikel 7.1 ska medlemsstaterna, när de fastställer om en störande effekt som avses i artikel 6.2 punkten c är betydande, beakta följande kriterier:

- a) Antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamhetsutövaren tillhandahåller.
- b) Den grad till vilken andra sektorer och undersektorer som anges i bilagan är beroende av den samhällsviktiga tjänsten i fråga.
- c) Vilken effekt incidenter skulle kunna ha på ekonomisk och samhällsrelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa, uttryckt i grad och varaktighet.
- d) Verksamhetsutövarens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna.
- e) Det geografiska område som skulle kunna påverkas av en incident, inbegripet eventuella gränsöverskridande konsekvenser, med

beaktande av den sårbarhet som är förknippad med graden av isole-
ring för vissa typer av geografiska områden, såsom öregioner, av-
lägsna områden eller bergsområden.

- f) Verksamhetsutövarens betydelse för upprätthållandet av en tillräck-
lig nivå på den samhällsviktiga tjänsten, med beaktande av till-
gången till alternativa sätt för att tillhandahålla den samhällsviktiga
tjänsten.

2.4.10 Stöd till kritiska verksamhetsutövare

Enligt artikel 10.1 ska medlemsstaterna stödja kritiska verksamhetsutövare
för att stärka deras motståndskraft. Stödet får innefatta utveckling av vägled-
ningsmaterial och metoder, stöd till anordnande av övningar för att testa de-
ras motståndskraft och tillhandahållande av rådgivning och utbildning för
kritiska verksamhetsutövares personal. Utan att det påverkar tillämpningen
av gällande regler för statligt stöd får medlemsstaterna tillhandahålla ekono-
miska resurser till kritiska verksamhetsutövare, om det är nödvändigt och
motiverat av mål av allmänt intresse.

2.4.11 Bakgrundskontroller

Enligt artikel 14.1 ska medlemsstaterna ange de villkor enligt vilka en kritisk
verksamhetsutövare, i vederbörligen motiverade fall och med beaktande av
medlemsstatens riskbedömning, får ansöka om bakgrundskontroller av per-
soner som

- a) innehar känsliga roller i eller till förmån för den kritiska verksamhets-
utövaren, särskilt när det gäller den kritiska verksamhetsutövarens
motståndskraft,
- b) är bemyndigade att direkt eller på distans få tillgång till den kritiska
verksamhetsutövarens lokaler eller dess informations- eller kontroll-
system, inbegripet när det gäller den kritiska verksamhetsutövarens
säkerhet,
- c) övervägs för rekrytering till tjänster som omfattas av de kriterier som
anges i led a eller b.

Enligt artikel 14.2 ska de ansökningar som avses i artikel 14.1 bedömas
inom en rimlig tidsram och hanteras i enlighet med nationell rätt och nation-
ella förfaranden samt relevant och tillämplig unionsrätt, inbegripet förord-
ning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU)
2016/680. Bakgrundskontroller ska vara proportionella och strikt begränsade
till vad som är nödvändigt. De ska utföras enbart i syfte att utvärdera en po-
tentiell säkerhetsrisk för den berörda kritiska verksamhetsutövaren.

Enligt artikel 14.3 ska en bakgrundskontroll enligt artikel 14.1 åt-
minstone:

- a) bekräfta identiteten på den person som är föremål för bakgrundskon-
trollen,
- b) kontrollera uppgifter ur kriminalregistret för den personen avseende
brott som är relevanta för en viss tjänst.

När de utför bakgrundskontroller ska medlemsstaterna använda det europe-
iska informationssystemet för utbyte av uppgifter ur kriminalregister i enlig-
het med de förfaranden som fastställs i rambeslut 2009/315/RIF och, i före-
kommande och tillämpliga fall, förordning (EU) 2019/816 för att inhämta
uppgifter ur kriminalregister som innehas av andra medlemsstater. De
centralmyndigheter som avses i artikel 3.1 i rambeslut 2009/315/RIF och i
artikel 3.5 i förordning (EU) 2019/816 ska besvara begäranden om sådana
uppgifter inom tio arbetsdagar från och med den dag då begäran togs emot i
enlighet med artikel 8.1 i rambeslut 2009/315/RIF.

2.4.12 Kritiska verksamhetsutövers riskbedömning

Enligt artikel 12.1 ska medlemsstaterna, utan hinder av den tidsfrist som anges i artikel 6.3 andra stycket, säkerställa att kritiska verksamhetsutövare gör en riskbedömning inom nio månader från mottagandet av den underrättelse som avses i artikel 6.3 och därefter när det är nödvändigt och minst vart fjärde år, på grundval av medlemsstaternas riskbedömningar och andra relevanta informationskällor, för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster, den så kallade riskbedömningen av kritiska verksamhetsutövare.

Enligt artikel 12.2 ska riskbedömningar av kritiska verksamhetsutövare innehålla en redogörelse för alla relevanta risker för naturolyckor och risker orsakade av människan som skulle kunna leda till en incident, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott enligt direktiv (EU) 2017/541. En riskbedömning av kritiska verksamhetsutövare ska beakta den grad till vilken andra sektorer som anges i bilagan är beroende av den samhällsviktiga tjänst som tillhandahålls av den kritiska verksamhetsutövaren och den grad till vilken den kritiska verksamhetsutövaren är beroende av samhällsviktiga tjänster som tillhandahålls av andra verksamhetsutövare i sådana andra sektorer, inbegripet i angränsande medlemsstater och tredjeländer i förekommande fall.

Om en kritisk verksamhetsutövare, i enlighet med skyldigheter som föreskrivs i andra rättsakter, har gjort andra riskbedömningar eller utarbetat dokument som är relevanta för dess riskbedömning av kritiska verksamhetsutövare får den använda dessa bedömningar och dokument för att uppfylla kraven i denna artikel. När den behöriga myndigheten utövar sina tillsynsfunktioner får den slå fast att en befintlig riskbedömning som gjorts av en kritisk verksamhetsutövare och som omfattar de risker och den beroendegrad som avses i första stycket i denna punkt helt eller delvis uppfyller skyldigheterna enligt denna artikel.

2.4.13 Kritiska verksamhetsutövers åtgärder för motståndskraft

Enligt artikel 13.1 ska medlemsstaterna säkerställa att kritiska verksamhetsutövare vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft, på grundval av den relevanta information som tillhandahålls av medlemsstaterna om medlemsstaternas riskbedömning samt resultatet av riskbedömningen av kritiska verksamhetsutövare, inbegripet åtgärder som är nödvändiga för att:

- a) förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning,
- b) säkerställa ett tillfredsställande fysiskt skydd av deras lokaler och kritiska infrastruktur, med vederbörlig hänsyn till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller,
- c) reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner,
- d) återhämta sig från incidenter, med vederbörlig hänsyn till åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten,
- e) säkerställa en ändamålsenlig hantering av personalsäkerhet, med vederbörlig hänsyn till åtgärder såsom fastställande av kategorier av personal som utför kritiska funktioner, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14 och fastställande av de kategorier av personer som måste genomgå

sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer,

- f) öka medvetenheten om de åtgärder som anges i leden a–e hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

Vid tillämpning av första stycket punkten e ska medlemsstaterna säkerställa att kritiska verksamhetsutövare beaktar externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner.

Enligt artikel 13.2 ska medlemsstaterna säkerställa att kritiska verksamhetsutövare har och tillämpar en plan för motståndskraft eller ett eller flera likvärdiga dokument med en beskrivning av de åtgärder som vidtagits enligt artikel 13.1. Om kritiska verksamhetsutövare har utarbetat dokument eller vidtagit åtgärder i enlighet med skyldigheter som anges i andra rättsakter som är relevanta för de åtgärder som avses i artikel 13.1 får de använda dessa dokument och åtgärder för att uppfylla kraven i artikel 13.2. När den behöriga myndigheten utövar sina tillsynsfunktioner får den slå fast att befintliga motståndskraftsstärkande åtgärder som vidtagits av en kritisk verksamhetsutövare och som på ett lämpligt och proportionerligt sätt adresserar de tekniska, säkerhetsmässiga och organisatoriska åtgärder som avses i artikel 13.1 helt eller delvis uppfyller skyldigheterna enligt artikel 13.2.

Enligt artikel 13.3 ska medlemsstaterna säkerställa att varje kritisk verksamhetsutövare utser en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna.

2.4.14 Rapporteringsskyldigheter

Enligt artikel 15.1 ska medlemsstaterna säkerställa att kritiska verksamhetsutövare utan onödigt dröjsmål lämnar in en anmälan till den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. Medlemsstaterna ska säkerställa att de kritiska verksamhetsutövarna, om det inte är operativt omöjligt för dem, lämnar in en första anmälan inom 24 timmar efter det att de 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 parametrar tas i beaktande:

- a) Antal och andel användare som berörs av störningen.
- b) Störningens varaktighet.
- c) Det geografiska område som påverkas av störningen, med beaktande av huruvida området är geografiskt isolerat.

Om en incident har eller kan ha en betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater ska de behöriga myndigheterna i de medlemsstater som berörs av incidenten anmäla den incidenten till kommissionen.

Enligt artikel 15.2 ska de anmälningar som avses i artikel 15.1 första stycket omfatta all tillgänglig information som är nödvändig för att den behöriga myndigheten ska kunna förstå incidentens art, orsak och möjliga konsekvenser, inbegripet eventuell information som krävs för att kunna fastställa incidentens eventuella gränsöverskridande verkningar. Sådana anmälningar ska inte medföra ett ökat ansvar för de kritiska verksamhetsutövarna.

Enligt artikel 15.3 ska den behöriga myndigheten, på grundval av den information som en kritisk verksamhetsutövare lämnar i den anmälan som avses i artikel 15.1, via den gemensamma kontaktpunkten informera den gemensamma kontaktpunkten i andra medlemsstater som 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. Gemensamma kontaktpunkter som skickar eller

tar emot information enligt första stycket ska i enlighet med unionsrätten eller nationell rätt behandla den informationen på ett sätt som respekterar dess konfidentialitet och skyddar den berörda kritiska verksamhetsutövarens säkerhet och kommersiella intressen.

Enligt artikel 15.4 ska den behöriga myndigheten, så snart som möjligt efter en anmälan enligt artikel 15.1, ge den berörda kritiska verksamhetsutövaren relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa den kritiska verksamhetsutövaren att reagera ändamålsenligt på incidenten i fråga. Medlemsstaterna ska informera allmänheten om de anser att det skulle ligga i allmänhetens intresse.

2.4.15 Standardisering

Enligt artikel 16 ska medlemsstaterna, för att främja ett enhetligt genomförande av direktivet, när det är användbart och utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationellt erkända standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft som är tillämpliga på kritiska verksamhetsutövare.

2.4.16 Tillsyn och efterlevnadskontroll

Enligt artikel 21.1 ska medlemsstaterna, för att bedöma om de verksamhetsutövare som medlemsstaterna har identifierat som kritiska verksamhetsutövare enligt artikel 6.1 fullgör de skyldigheter som fastställs i direktivet, säkerställa att de behöriga myndigheterna har befogenheter och medel för att:

- a) genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som den kritiska verksamhetsutövaren använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av de åtgärder som vidtagits av kritiska verksamhetsutövare i enlighet med artikel 13,
- b) utföra eller beställa revisioner av kritiska verksamhetsutövare.

Enligt artikel 21.2 ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenheter och medel för att, när så är nödvändigt för att fullgöra deras uppgifter enligt direktivet, kräva att verksamhetsutövare enligt cybersäkerhetsdirektivet som medlemsstaterna har identifierat som kritiska verksamhetsutövare enligt motståndskraftsdirektivet, inom en rimlig tidsfrist, som fastställs av dessa myndigheter, lämnar:

- a) den information som är nödvändig för att bedöma om de åtgärder som verksamhetsutövarna har vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 13,
- b) bevis på att de åtgärderna faktiskt har genomförts, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad revisor som har valts av verksamhetsutövaren och som har utförts på verksamhetsutövarens bekostnad.

När de behöriga myndigheterna begär denna information ska de ange syftet med kravet och specificera vilken information som krävs.

Enligt artikel 21.3 får den behöriga myndigheten, utan att det påverkar möjligheten att ålägga sanktioner i enlighet med artikel 22, efter de tillsynsåtgärder som avses i artikel 21.1 eller den bedömning av information som avses i artikel 21.2, beordra de berörda kritiska verksamhetsutövarna att vidta de åtgärder som är nödvändiga och proportionella för att avhjälpa konstaterade överträdelser av direktivet, inom en rimlig tidsfrist som fastställs av de myndigheterna, och att lämna information om de åtgärder som har vidtagits till de myndigheterna. Sådana förelägganden ska framför allt ta hänsyn till hur allvarlig överträdelsen är.

Enligt artikel 21.4 ska medlemsstaterna säkerställa att de befogenheter som anges i artikel 21.1–3 endast kan utövas om de omfattas av lämpliga

skyddsåtgärder. Sådana skyddsåtgärder ska särskilt garantera att befogenheterna utövas på ett objektivt, öppet och proportionerligt sätt och att de berörda kritiska verksamhetsutövarnas rättigheter och legitima intressen, såsom skyddet av handels- och affärshemligheter, skyddas på vederbörligt sätt, däribland rätten att höras, rätten till försvar och rätten till rättslig prövning inför en oberoende domstol.

Sanktioner

Enligt artikel 22 ska medlemsstaterna fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 17 oktober 2024 samt utan dröjsmål eventuella ändringar som berör dem.

2.5 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) antogs den 27 april 2016 och reglerar utöver dataskydd även cybersäkerhet i förhållande till behandlingen av personuppgifter.

Enligt den allmänna dataskyddsförordningens skäl 39 bör personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

Enligt förordningens skäl 49 utgör behandling av personuppgifter ett berättigat intresse för berörd personuppgiftsansvarig i den mån den är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet. Det vill säga förmågan hos ett nät eller ett informationssystem att vid en viss tillförlitlighetsnivå tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande vilket äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda personuppgifter och säkerheten hos beslätade tjänster som tillhandahålls av, eller är tillgängliga via, dessa nät och system, av myndigheter, incidenthanteringsorganisationer, enheter för hantering av datasäkerhetsincidenter, tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av säkerhetsteknik och säkerhetstjänster. Detta skulle exempelvis kunna innefatta att förhindra obehörigt tillträde till elektroniska kommunikationsnät och felaktig kodfördelning och att sätta stopp för överbelastningsattacker och skador på datasystem och elektroniska kommunikationssystem.

Enligt förordningens skäl 83 bör personuppgiftsansvariga eller personuppgiftsbiträden, för att upprätthålla säkerheten och förhindra behandling som bryter mot förordningen, utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem. Åtgärderna bör säkerställa en lämplig säkerhetsnivå, inbegripet konfidentialitet, med beaktande av den senaste utvecklingen och genomförandekostnader i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas. Vid bedömningen av datasäkerhetsrisken bör även de risker vilka personuppgiftsbehandling medför beaktas, såsom förstörelse, förlust eller ändringar genom olyckshändelse eller otillåtna handlingar eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförs, lagrats eller på annat sätt behandlats, framför allt när denna kan medföra fysisk, materiell eller immateriell skada.

Enligt förordningens artikel 5.1 f ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet

skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

Enligt förordningens artikel 25.1 ska den personuppgiftsansvarige, med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, vilka är utformade för ett effektivt genomförande av dataskyddsprinciper, såsom uppgiftsminimering, och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i förordningen uppfylls och den registrerades rättigheter skyddas.

Enligt förordningens artikel 32.1 ska den personuppgiftsansvarige och personuppgiftsbiträdet, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt:

- a) pseudonymisering och kryptering av personuppgifter,
- b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
- c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt den allmänna dataskyddsförordningens artikel 32.2 ska vidare särskild hänsyn tas till de risker som behandling medför vid bedömningen av lämplig säkerhetsnivå, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Enligt cybersäkerhetsdirektivets artikel 2.12 jämte motståndskraftsdirektivets artikel 1.9 påverkar inte direktiven den allmänna dataskyddsförordningens tillämpning.

2.6 Kodexdirektivet

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (nedan kallat *kodexdirektivet*) antogs den 11 december 2018, har genomförts i riket, främst genom lagen om elektronisk kommunikation, och föreskriver närmare reglering av bland annat elektroniska kommunikationsnät och kommunikationstjänster.

Enligt kodexdirektivets artikel 40.1 ska tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar näts och tjänsters säkerhet. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en nivå på säkerheten som är lämplig i förhållande till den föreliggande risken. I synnerhet ska åtgärder, inbegripet kryptering när så är lämpligt, vidtas för att förhindra och minimera säkerhetsincidenters inverkan på användare och på andra nät och tjänster.

Enligt direktivets artikel 40.2 ska tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska

kommunikationstjänster utan onödigt dröjsmål meddela den behöriga myndigheten om säkerhetsincidenter som har haft en betydande påverkan på driften av nät och tjänster. För att fastställa hur betydande påverkan en säkerhetsincident har ska särskilt följande parametrar, när sådana finns tillgängliga, beaktas:

- a) a) Det antal användare som påverkas av säkerhetsincidenten.
- b) Hur länge säkerhetsincidenten varar.
- c) Hur stort det geografiska område som påverkas av säkerhetsincidenten är.
- d) Den utsträckning i vilken nätverkets eller tjänstens funktion påverkas.
- e) Den utsträckning i vilken ekonomisk och samhällelig verksamhet påverkas.

Enligt direktivets artikel 40.3 ska tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, om det föreligger ett särskilt och betydande hot om en säkerhetsincident i sådana nät eller tjänster, informerar de av sina användare som kan komma att påverkas av ett sådant hot om eventuella skydds- eller motåtgärder som användarna kan vidta. Om så är lämpligt ska tillhandahållarna även informera sina användare om själva hotet.

Enligt artikel 41.1 ska de behöriga myndigheterna i syfte att genomföra artikel 40 ha befogenheter att utfärda bindande instruktioner, däribland sådana som rör de åtgärder som krävs för att avhjälpa en säkerhetsincident eller förhindra att en sådan uppstår när ett betydande hot har identifierats och tidsfrister för genomförande, till tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

Enligt direktivets artikel 41.2 ska de behöriga myndigheterna ha befogenheter att kräva av tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster att de:

- a) tillhandahåller den information som behövs för att kunna bedöma säkerheten i deras nät och tjänster, inbegripet dokumenterade säkerhetspolicier, och
- b) underkastar sig en säkerhetsgranskning som utförs av ett kvalificerat oberoende organ eller en behörig myndighet och gör resultatet av granskningen tillgängligt för den behöriga myndigheten; kostnaderna för säkerhetsgranskningen ska betalas av tillhandahållaren.

Den berörda behöriga myndigheten ska vid behov informera de behöriga myndigheterna i övriga medlemsstater och Enisa. Den berörda behöriga myndigheten kan informera allmänheten eller kräva att tillhandahållarna gör det, om den slår fast att ett avslöjande av säkerhetsincidenten ligger i allmänhetens intresse. En gång om året ska den berörda behöriga myndigheten lämna in en sammanfattande rapport till kommissionen och Enisa om de anmälningar vilka har kommit in och de åtgärder som vidtagits i enlighet med artikeln.

Enligt direktivets artikel 41.3 ska behöriga myndigheterna ha alla nödvändiga befogenheter för att undersöka fall av bristande efterlevnad och hur detta påverkar nätens och tjänsternas säkerhet.

Cybersäkerhetsdirektivet medförde ändringar av artikel 40 och 41 i kodedirektivet, i syfte att harmonisera de båda regelverken.

2.7 Komparativ utblick

2.7.1 Sverige

2.7.1.1 Allmänt

Sveriges regering beslöt den 23 februari 2023 i ett kommittédirektiv, Dir. 2023:30, att utse en särskild utredare som skulle föreslå de anpassningar av svensk rätt som är nödvändiga för att cybersäkerhetsdirektivet och motståndskraftsdirektivet skulle kunna genomföras i den svenska rättsordningen, för redovisning senast den 23 februari 2024.

I kommittédirektivet ingick vidare ett antal särskilda direktiv till utredaren kopplade till cybersäkerhetsdirektivet, som att den skulle utreda vilka aktörer som ska omfattas av regleringen, rollfördelningen mellan svenska myndigheter, krav på aktörerna, tillsynsmyndigheternas befogenheter och föreslå författningsförslag. I förhållande till motståndskraftsdirektivet uppställdes även där särskilda direktiv till utredaren, som att den skulle utreda rollfördelningen mellan svenska myndigheter, sättet för identifiering av kritiska verksamhetsutövare, kravställningen på de kritiska verksamhetsutövarna, utformningen av systemet för bakgrundskontroller, tillsynsmyndigheternas befogenheter och föreslås författningsförslag. Gemensamt för de båda direktiven var även att utredaren fick särskilda direktiv om att se över förhållandet till säkerhetsskyddsregleringen, förhållandet till annan unionsrättslig och nationell reglering, förhållandet till offentlighets- och sekretessregleringen och konsekvensbeskrivningar, samt vid behov lämna förslag till författningsändringar.

Genom tilläggsdirektiv, Dir. 2024:3, av den 11 januari 2024, förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av motståndskraftsdirektivet.

2.7.1.2 Cybersäkerhetsdirektivet

Utredningen överlämnade i mars 2024 sitt delbetänkande, *Nya regler om cybersäkerhet*, SOU 2024:18, om hur cybersäkerhetsdirektivet ska genomföras i svensk rätt. Utredningens övergripande slutsats är att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt, varvid ett normalt språkbruk ska eftersträvas. I linje med denna slutsats valde Sverige, bland annat, att ersätta begreppet entitet med det mer begripliga och i svensk rättsordning nyttjade uttrycket verksamhetsutövare. Utredningen drar även slutsatsen att direktivet bör införlivas genom att en särskild cybersäkerhetslag stiftas för genomförandet, i enlighet med förfarandet för det gamla cybersäkerhetsdirektivet. Cybersäkerhetslagen föreslås vidare att kompletteras med en föreslagen förordning om cybersäkerhet, vilken främst föreslås innehålla kompletterande detaljreglering rörande verksamhetsutövaras utpekade myndigheter samt deras uppgifter. Utredningen föreslår även, med vissa undantag, inte några skyldigheter utöver vad som följer av direktivet.

Utredningen föreslår vidare att cybersäkerhetslagen ska gälla för de flesta statliga myndigheter i Sverige, med regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen och domstolarna är undantagna. Detsamma gäller för sammanlagt 16 myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning. Utredningen föreslår dock att samtliga regioner och kommuner ska omfattas av lagens krav, region- och kommunfullmäktige undantagna, samt inkluderande lärosäten med examenstillstånd. Cybersäkerhetslagen föreslås vidare gälla för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet, men där den delen inte utgör en väsentlig andel, samt enskilda verksamhetsutövare, vilka bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten

eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet. Detsamma gäller för verksamhetsutövare som redan omfattas av skyldigheter med motsvarande verkan som kraven i cybersäkerhetslagen, exempelvis för finansiella verksamhetsutövare som omfattas av motståndskraftsförordningen för finanssektorn.

Utredningen föreslår även att det fortsatt ska finnas en tillsynsmyndighet för varje sektor, vilka dock utökas i förhållande till de nya sektorerna och därmed blir elva totalt, till skillnad från de tidigare sex. Myndigheten för samhällsskydd och beredskap (nedan kallad *MSB*) föreslås även att fortsatt leda ett samarbetsforum där tillsynsmyndigheterna ingår, i syfte att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Utredningen föreslår att *MSB* fortsatt ska utgöra gemensam kontaktpunkt, mot bakgrund av dess nuvarande uppgifter och uppgiften att stödja och samordna arbetet med samhällets informationssäkerhet. Utredningen föreslår att *MSB*, mot bakgrund av att myndigheten i dag har uppdrag och kompetens som gör att den fortsatt ska utgöra enhet för hantering av it-säkerhetsincidenter samt cyberkrishanteringsmyndighet i Sverige. I utredningens förslag ingår vidare att tillsynsmyndigheterna utses av regeringen genom förordning.

Utredningen räknar vidare med inledande ökade kostnader för tillsynsmyndigheterna avseende identifiering av de verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionsnivån för tillsynsverksamheten.

Utredningen föreslår att författningsförslagen ska träda i kraft den 1 januari 2025.

2.7.1.3 Motståndskraftsdirektivet

Utredningen överlämnade i september 2024 sitt slutbetänkande, Motståndskraft i samhällsviktiga tjänster, SOU 2024:64, om hur motståndskraftsdirektivet ska genomföras i svensk rätt. Utredningen föreslår att motståndskraftsdirektivet ska genomföras genom en ny lag, lagen om motståndskraft hos kritiska verksamhetsutövare och föreslår inte att några ytterligare skyldigheter utöver vad som följer av direktivet ska införas.

Utredningen föreslår att regelverket ska tillämpas på enskilda och offentliga verksamhetsutövare som tillhandahåller en samhällsviktig tjänst som omfattas av bilagan till direktivet. Vidare krävs att verksamhetsutövaren har identifierats som kritisk av tillsynsmyndigheten. Tillsynsmyndigheterna ska genom beslut identifiera kritiska verksamhetsutövare inom sina tillsynsområden. I förslaget görs vissa undantag från lagens tillämpningsområde. Lagen gäller inte för sådant som regleras i förslaget till lag om cybersäkerhet och inte heller om det i annan författning finns bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroll och incidentrapportering om kraven har minst motsvarande verkan. Lagen gäller inte heller för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen eller Sveriges domstolar. Lagen gäller inte för statliga myndigheter som till övervägande del bedriver brottsbekämpning eller säkerhetskänslig verksamhet.

Utredningen föreslår att den tillsynsmyndighet som är tillsynsmyndighet enligt den föreslagna lagen om cybersäkerhet även blir tillsynsmyndighet enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Ett fåtal tillsynsmyndigheter har fått en ny undersektor eller kategori av verksamhetsutövare. Vidare ingår i sektorn offentlig förvaltning endast statliga myndigheter. *MSB* ska leda ett samarbetsforum där tillsynsmyndigheterna ingår för att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. Myndigheten för samhällsskydd och beredskap ska vara gemensam

kontaktpunkt. Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa det gränsöverskridande samarbetet med gemensamma kontaktpunkter i andra medlemsstater och med kommissionen. Nivåerna på sanktionsavgiften föreslås vara desamma som för väsentliga verksamhetsutövare i lagen om cybersäkerhet. Det innebär att sanktionsavgiften för enskilda kritiska verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av två procent av den kritiska verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller 10 000 000 euro. För offentliga kritiska verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst till 10 000 000 kronor.

Utredningen föreslår att sekretesskyddet ska stärkas och föreslår att en ny bestämmelse om sekretess införs i 18 kap. OSL för uppgift i incidentrapporter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident. Bestämmelsen föreslås få ett omvänt skaderekvisit och rätten att meddela och offentliggöra uppgifterna begränsas. Vidare föreslås att diarium över incidenter hos rapporterade myndigheter, tillsynsmyndigheter och MSB ska kunna omfattas av sekretess. För att MSB och tillsynsmyndigheterna ska kunna lämna ut uppgifter som härrör från andra medlemsstater och EU:s institutioner och som omfattas av sekretess till varandra, föreslår utredningen en ny sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. När det gäller bakgrundskontroller föreslås en bestämmelse om tystnadsplikt för uppgifter som förekommer i angelägenheter som avser bakgrundskontroll i den nya lagen. Sekretesskyddet för uppgifter som tillsynsmyndigheten kommer att hantera behöver kompletteras när det gäller uppgifter som rör enskilda affärs- eller driftsförhållanden.

Utredningen föreslår att lagen om motståndskraft hos kritiska verksamhetsutövare och tillhörande förordning ska träda i kraft den 1 augusti 2025. Förslagen i offentlighets- och sekretesslagen och offentlighets- och sekretessförordningen som gäller lagen om cybersäkerhet föreslås träda i kraft den 1 januari 2025. Övriga förslag föreslås träda i kraft den 1 augusti 2025.

2.7.2 Finland

2.7.2.1 Allmänt

Statsrådets kommunikationsministerium inrättade i januari 2023 en arbetsgrupp till stöd för det nationella genomförandet av cybersäkerhetsdirektivet i januari 2023, även kallad huvudarbetsgruppen. Huvudarbetsgruppen hade till uppgift att bedöma vilka lagstiftningsändringar som behövs för genomförandet av direktivet och att gemensamt utarbeta en regeringsproposition om de behövliga lagstiftningsändringarna. Kommunikationsministeriet inrättade också en underarbetsgrupp till huvudarbetsgruppen och den inriktade sig på offentlig förvaltning, även kallad underarbetsgruppen. Underarbetsgruppen hade till uppgift att bedöma och bereda genomförandet av skyldigheterna i cybersäkerhetsdirektivet med avseende på sektorn offentlig förvaltning, vilken omfattas av direktivets tillämpningsområde.

Statsrådets inrikesministerium tillsatte den 7 december 2022 ett lagstiftningsprojekt (VN/18947/2022) för identifiering av kritiska aktörer och förbättring av den kritiska infrastrukturens motståndskraft, vilket skulle avslutas den 31 december 2024. I samband med stärkandet och skyddet av den nationellt viktiga infrastrukturens funktion skulle projektet utarbeta ett förslag i form av en regeringsproposition till en allmän lag eller ramlag om identifiering av kritisk infrastruktur och förbättrande av motståndskraften samt förslag till behövliga ändringar av den sektorsspecifika speciallagstiftningen, vilka samtidigt genomför motståndskraftsdirektivet. I enlighet med beslutet om tillsättande skulle varje ministerium inom sitt förvaltningsområde ansvara för att kartlägga nuläget och bereda eventuell ny sektorsspecifik

lagstiftning. I projektet ansvarade inrikesministeriet för beredningen av ramlagen eller den allmänna lagen och lagstiftningen om tillsynsarrangemang för åtgärder för motståndskraft mot kriser.

Projektets arbetsgrupp skulle särskilt utreda nuläget i lagstiftningen och eventuella befintliga förfaranden för att identifiera och övervaka kritiska aktörer och stödja deras åtgärder för motståndskraft mot kriser, utarbeta förslag till hur myndighetsfunktioner och myndighetstillsyn enligt motståndskrafts-direktivet ska organiseras centralt under statsrådet, utarbeta förslag till stöd för aktörer i enlighet med direktivet, granska de frågor som ska tas upp på nationell nivå, exempelvis nationell säkerhet, sektorer som är kritiska för försvaret och skydd av geografisk information, utvärdera synergier mellan de nya resiliensuppdrag som Nato förutsätter och organisationen av motståndskraftsverksamheten och utarbeta ett förslag till ny ramlag och ändringar i den sektorspecifika lagstiftningen i form av en regeringsproposition.

2.7.2.2 Cybersäkerhetsdirektivet

Statsrådet lämnade den 23 maj 2024 sin proposition, RP 57/2024, till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet.

I propositionen föreslås att det stiftas en ny allmän lag om hantering av cybersäkerhetsrisker. I fråga om den offentliga sektorn föreslås att det ska föreskrivas särskilt om skyldigheterna även i lagen om informationshantering inom den offentliga förvaltningen. Samtidigt upphävs i flera sektorspecifika speciallagar genomförandebestämmelserna för det tidigare direktivet om nät- och informationssäkerhet. Enligt förslaget ska cybersäkerhetsdirektivet genomföras enligt miniminivån, direktivnära och genom omskrivning, samt genom ett fullt utnyttjande av det nationella handlingsutrymmet.

Propositionens föreslår att kommuner och aktörer inom utbildningssektorn undantas från förslagens tillämpningsområden. Helsingfors stad omfattas dock till den del den sköter uppgifter som hör till organiseringsansvaret för välfärdsområden. Kommunerna undantas dock inte i sin helhet, utan de delar av organisationen vilka bedriver verksamhet vilken omfattas av tillämpningsområdet ska omfattas av förslaget till allmän lag. Bedömningen av verksamhetens storlek ska dock enbart ske med beaktande av storleken på den del av organisationen vilken bedriver aktuell verksamhet och tillämpningsområdet ska följaktligen inte heller utsträckas till att omfatta hela kommunen. På grund av skäl som gäller nationell säkerhet, allmän säkerhet, försvaret eller myndigheter inom sektorn brottsbekämpning samt tjänsteproducenter av säkerhetsnät och användning av tjänsterna gäller föreslås det inte att dessa aktörer ska omfattas av tillämpningsområdet för regleringen. Vidare undantar förslaget till allmän lag aktörer vilka enbart bedriver av tillämpningsområdet omfattad verksamhet i ringa eller sporadisk omfattning.

Enligt propositionens föreslås den sedan tidigare sektorsvis uppdelade modellen med sektorspecifika tillsynsmyndigheter att fortsättningsvis gälla, varav bland annat Transport- och kommunikationsverkets utses till tillsynsmyndighet för den offentliga förvaltningen samt dess cybersäkerhetscenter utses till gemensam kontaktpunkt. Samtliga utpekade tillsynsmyndigheter utses vidare till cyberkrishanteringsmyndigheter, varav Transport- och kommunikationsverkets cybersäkerhetscenter utses till samordnande cyberkrishanteringsmyndighet. I propositionen föreslås även att Transport- och kommunikationsverkets cybersäkerhetscenter ska utgöra enhet, därmed tillika samordnande enhet, för hantering av it-säkerhetsincidenter.

Propositionen föreslår att författningarna ska träda i kraft den 18 oktober 2024.

2.7.2.3 Motståndskraftsdirektivet

Inrikesministeriet skickade den 26 februari 2024 ut ett utkast till proposition med förslag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft samt till vissa andra lagar på remiss.

I utkastet till proposition föreslås att det stiftas en ny allmän lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. Enligt utkastet till proposition ska direktivet genomföras utan nationella utvidgningar. I enlighet med direktivet innehåller författningsförslaget en process för identifiering av kritiska aktörer och gemensamma kriterier för identifieringen samt skyldigheter för kritiska aktörer att stärka sin motståndskraft och sin kapacitet att tillhandahålla samhällsviktiga tjänster åtminstone i enlighet med minimikraven i direktivet. De aktörer som omfattas av tillämpningsområdet för den allmänna lagen definieras i enlighet med tillämpningsområdet för motståndskraftsdirektivet. Vid genomförandet av direktivet föreslås därmed inga nationella utvidgningar av tillämpningsområdet.

I utkastet föreslås att på statsrådsnivå ska inrikesministeriet sköta samordningen samt den allmänna styrningen av verksamheten och utses därmed till behörig myndighet enligt direktivet. Uppdelningen på sektorsspecifika tillsynsmyndigheter bibehålls i övrigt. Tillsynsmyndigheter är således de myndigheter som bestäms enligt den sektorsspecifika speciallagstiftningen, bland annat Transport- och kommunikationsverket. Den under arbets- och näringsministeriet lydande Försörjningsberedskapscentralen tilldelas rollen som gemensam kontaktpunkt, samt underställs inrikesministeriet när det gäller den operativa styrningen i fråga om uppgifterna som föreskrivs i författningsförslaget. För statsrådets lägescentral föreslås en uppgift att förmedla anmälningar om incidenter med betydande verkan till kommissionen i enlighet med inrikesministeriets rapport.

I utkastet till proposition föreslås det sammanhängande ändringar i bland annat säkerhetsutredningslagen, mot bakgrund av bakgrundskontrollerna och genomförandet av direktivet och om utlämnande av sådana uppgifter mellan Finland och övriga medlemsstater.

Enligt utkastet till proposition har statsrådet tillsatt en arbetsgrupp för att bereda en totalreform av beredskapslagen, och vid genomförandet av motståndsdirektivet har arbetsgruppens begäran om utlåtande om en promemoria om skyldigheten enligt beredskapslagen att vidta förberedelser beaktats. I arbetsgruppens promemoria betonar den förutom beredskapen för undantagsförhållanden också behovet av beredskap för störningar som är lindrigare än undantagsförhållanden. I promemorian konstateras vidare att trots att det föreskrivs om beredskap för störningar under normala förhållanden i flera sektorsspecifika lagar ingår i den finländska lagstiftningen ingen allmän bestämmelse som uttryckligen förpliktar den offentliga förvaltningen att förbereda sig för störningar som inte överskrider tröskeln för undantagsförhållanden. Arbetsgruppen för beredskapslagen anser i promemorian att detta är en brist i lagstiftningen och att den allmänna beredskapsskyldigheten enligt beredskapslagen bör gälla beredskap såväl för undantagsförhållanden som för lindrigare störningar. Det är inte ändamålsenligt att på nationell nivå utvidga motståndskraftsregleringen till att omfatta nya aktörer inom den offentliga sektorn utöver dem som anges i motståndskraftsdirektivet.

Någon proposition har i skrivande stund inte överlämnats till riksdagen ifrån Statsrådet.

2.8 Sammanfattande bedömning

Landskapsregeringen bedömer att Åland måste genomföra direktiven om cybersäkerhet och motståndskraft, till den del som dessa reglerar rättsområden

som faller in under Ålands lagstiftningsbehörighet, se närmare redogörelse av lagstiftningsbehörigheten under avsnitt 4 nedan.

Landskapsregeringen bedömer att ett antagande av en landskapslag, vilken tillämpliggör rikets genomförande på Åland, det vill säga en så kallad blankettreglering, inte är en för Åland och berörda verksamhetsutövare lämplig väg att välja. Rikets genomförande av de aktuella direktivens föregångare är utfördelat på ett större antal speciallagar. Rikets genomförande av aktuella direktiv justerar och kompletterar denna genom ett införande av två nya allmänna lagar, en för respektive direktiv. Rikets genomförande innebär därmed en delvis fortsättning på den sektorsspecifika uppdelningen, vilken även reflekteras i valet av tillsynsmodell, där sektorsspecifika myndigheter tilldelas tillsynsansvaret inom sitt respektive sakområde. De allmänna lagarna i genomförandet inbegriper vidare ett antal hänvisningar till rikets speciallagstiftning och definitioner i densamma, vilken inte alltid har en motsvarighet inom landskapet inom ramen för dess lagstiftningsbehörighet. Vidare har genomförandet av cybersäkerhetsdirektivets uppdelats i en offentlig och enskild del, där delar av regleringen av offentliga verksamhetsutövare sker inom ramen för lagen om informationshantering inom den offentliga förvaltningen (FFS 906/2014). Rikets genomförande förefaller vidare innehålla en del tveksamma juridiska överväganden avseende direktivets korrekta genomförande. En blankettreglering vilken gör rikets genomförande tillämpligt inom landskapet kan därmed förväntas försvåra de berörda åländska verksamhetsutövarnas överblick över genomförandet och därmed deras förmåga att ta till sig och tillämpa densamma. Ett blankettgenomförande inom landskapet kan vidare förväntas leda till ett mer omfattande lagberedningsarbete än om en helt ny och sammanhållen lag bereds.

Landskapsregeringen konstaterar vidare att direktiven har överlappande tillämpningsområden och nyttjar likartade regleringsinstrument, med därmed sammanhängande potential till synergieffekter. Landskapsregeringen bedömer därmed att åländska enskilda och offentliga verksamhetsutövare, vilka omfattas av direktivens tillämpningsområde, till följd av tillämpningsområdenas överlappning, skulle tjänas av att en sammanhållen allmän lag stiftas för genomförandet av de båda direktiven. Verksamhetsutövarna skulle vidare tjänas av att genomförandet, liksom de svenska författningsförslagen och till skillnad från de direktivnära genomförandena i riket, sker genom omskrivning, samt att det utformas utifrån den systematik och terminologi som normalt brukas i åländsk rätt, varvid ett normalt språkbruk eftersträvas. Verksamhetsutövarna skulle vidare tjänas av att det åländska genomförandet, till skillnad från det svenska, i huvudsak regleras i lag och inte i förordning, samtidigt som detta tillgodoser grundlagens och självstyrelselagens krav på lagreglering av grunderna för individens rättigheter och skyldigheter frågor som hör till området för lag.

Landskapsregeringen bedömer vidare att Åland, till följd av sina särskilda förhållanden, skulle tjänas bäst av att såväl tillämpningsområdet som kravställningen på olika typer av verksamhetsutövare inte överstiger den i direktiven föreskrivna miniminivån och att det nationella handlingsutrymmet nyttjas fullt ut i detta avseende.

Landskapsregeringen förordar vidare en tillsynsmodell, annan än den som har inrättats i såväl riket som i Sverige, enligt vilken myndighetsansvaren i direktiven koncentreras till en och samma centrala myndighet på Åland, i detta fall landskapsregeringen, varav åtminstone cybersäkerhetsansvaret i praktiken bör falla på dess digitaliseringsenhet.

3. Landskapsregeringens förslag och syften

Landskapsregeringen föreslår att det stiftas en ny allmän landskapslag om cybersäkerhet och motståndskraft. Genom den föreslagna lagen genomförs

cybersäkerhets- och motståndskraftsdirektiven på Åland. Syftet med det gemensamma genomförandet är att ge berörda verksamhetsutövare och tillsynsmyndigheten ett samlat, tydligt och enhetligt regelverk att förhålla sig till, vilket förväntas främja regleringens genomslag, en enhetlig tillämpning och en effektiv tillsyn och efterlevnadskontroll.

Den föreslagna lagens tillämpningsområde är 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.

I enlighet med den föreslagna lagens kapitelindelning föreskrivs i lagen om allmänna bestämmelser, lagens tillämpningsområde, klassificering, identifiering och informering av verksamhetsutövare, kritiska verksamhetsutövares skyldigheter, väsentliga och viktiga verksamhetsutövares skyldigheter, cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter, landskapsregeringens informationsansvar, tillsyn och efterlevnadskontroll samt särskilda bestämmelser.

Den föreslagna lagens 1 kap. föreskriver dess allmänna bestämmelser. I kapitlet anges lagens syften och införs definitioner, vilka såväl syftar till att genomföra direktivens definitioner som att underlätta lagens tillämpning och hänvisningar till rikslagstiftningen inom ramen för rikets lagstiftningsbehörighet.

I den föreslagna lagens 2 kap. föreskrivs om lagens tillämpningsområde. I kapitlet definieras omfattade verksamhetsutövare, avgränsningar av tillämpningsområdet, förhållandet till annan lagstiftning samt regleras tillämpligheten i förhållande till jurisdiktion, territorialitet och gränsöverskridande verksamhetsutövare.

I den föreslagna lagens 3 kap. föreskrivs om klassificering, identifiering och informering av verksamhetsutövare. I kapitlet regleras hur verksamhetsutövare klassificeras på objektiva grunder respektive identifieras genom beslut av landskapsregeringen utifrån subjektiva såväl som objektiva kriterier samt vilken information som verksamhetsutövare respektive landskapsregeringen ska tillhandahålla i samband med detta förfarande.

I den föreslagna lagens 4 kap. föreskrivs om kritiska verksamhetsutövares skyldigheter. I kapitlet regleras kritiska verksamhetsutövares skyldighet att genomföra en riskbedömning, vidta åtgärder och ta fram en plan för motståndskraft, påförs incidentrapporteringskyldigheter samt ges möjlighet att ansöka om säkerhetsutredning, uppmuntras nyttja standarder och påförs vissa skyldigheter kopplade till rådgivande uppdrag.

I den föreslagna lagens 5 kap. föreskrivs om väsentliga och viktiga verksamhetsutövares skyldigheter. I kapitlet regleras väsentliga och viktiga verksamhetsutövares skyldighet för dess ledning, krav på utbildning av ledning och personal, skyldighet vidta åtgärder och ta fram strategier för cybersäkerhet, påförs incidentrapporteringskyldigheter samt ges möjlighet att frivilligt rapportera om cybersäkerhetsincidenter, cyberhot och tillbud samt uppmuntras nyttja standarder europeiska ordningar för cybersäkerhetscertifiering.

I den föreslagna lagens 6 kap. föreskrivs om cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter. I kapitlet utpekas landskapsregeringen som cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter samt påförs vissa krav och uppgifter i samband med detta.

I den föreslagna lagens 7 kap. föreskrivs om landskapsregeringens informationsansvar. I kapitlet föreskrivs om landskapsregeringens skyldigheter i förhållande till inrättandet av arrangemang för frivilligt informationsutbyte, samt informationsansvar vid incidenter och cybersäkerhetsincidenter.

I den föreslagna lagens 8 kap. föreskrivs om tillsyn och efterlevnadskontroll. I kapitlet utpekas landskapsregeringen som tillsynsmyndighet enligt

lagen samt föreskrivs närmare om nationellt som internationellt samråd och myndighetssamarbete, stöd till verksamhetsutövare, skyldigheter kopplade till rådgivande uppdrag och sakkunnigbedömningar, befogenheter och skyldigheter kopplade till tillsyn och efterlevnadskontroll, sekretessbrytande bestämmelser, internationell handräckning, befogenhet att utfärda viten samt hot om tvångsutförande och avbrytande, befogenhet att utfärda administrativa påföljdsavgifter samt möjlighet för berörda att besvara sig emot landskapsregeringens beslut.

I den föreslagna lagens 9 kap. föreskrivs om särskilda bestämmelser. I kapitlet återfinns en ikraftträdandebestämmelse.

4. Lagstiftningsbehörighet

4.1 Allmänt

Enligt 1 § självstyrelselagen har landskapet Åland självstyrelse enligt vad som särskilt stadgas i självstyrelselagen. Enligt 59b § 1 mom. självstyrelselagen är lagstiftningsbehörigheten och behörigheten i förvaltningsärenden, när åtgärder vidtas i Finland med anledning av beslut vilka har fattats inom Europeiska unionen, fördelad mellan landskapet och riket på det sätt som följer av självstyrelselagen. Enligt 59b § 2 mom. självstyrelselagen ska riksmyndigheter, i samråd med landskapsmyndigheter, vidta åtgärder i ett förvaltningsärende där unionsrätten endast tillåter att en nationell åtgärd kan vidtas när behörigheten är delad mellan landskapet och riket. Enligt 59b § 3 mom. självstyrelselagen ska riket utse en förvaltningsmyndighet om unionsrätten föreskriver att endast en nationell sådan ska utses.

Enligt 18 § 1, 4, 6, 10, 12–16, 20–22 och 25–27 punkterna självstyrelselagen har landskapet lagstiftningsbehörighet i fråga om lagtingets organisation, landskapsregeringen och under denna lydande myndigheter och inrättningar, kommunernas förvaltning, allmän ordning och säkerhet, med de undantag som nämns i 27 § 27, 45 och 35 punkterna, brand- och räddningsväsendet, natur- och miljövård, vattenrätt, hälso- och sjukvården, med de undantag som stadgas i 27 § 24, 29 och 30 punkterna, socialvården, undervisning, arkiv- och biblioteksväsendet, med det undantag som stadgas i 27 § 39 punkten, jord- och skogsbruk, styrning av lantbruksproduktionen, jakt och fiske, styrning av fiskerinäringen, postväsendet samt rätt att utöva rundradio- och televisionsverksamhet inom landskapet, med de begränsningar som följer av 27 § 4 punkten, vägar och kanaler, vägtrafik, spårbunden trafik, båttrafik, farleder för den lokala sjötrafiken, näringsverksamhet, med beaktande av vad som stadgas i 11 §, 27 § 2, 4, 9, 12–15, 17–19, 26, 27, 29–34, 37 och 40 punkten samt 29 § 1 mom. 3–5 punkterna, beläggande med straff och storleken av straff inom rättsområden som hör till landskapets lagstiftningsbehörighet, utsättande och utdömande av vite samt användning av andra tvångsmedel inom rättsområden som hör till landskapets lagstiftningsbehörighet samt övriga angelägenheter som enligt grundsatserna i självstyrelselagen ska hänföras till landskapets lagstiftningsbehörighet.

Enligt 27 § 8, 10, 12–14, 18–19, 22, 23, 28, 30, 34, 40, och 42 punkterna självstyrelselagen har riket lagstiftningsbehörighet i fråga om bolag och andra privaträttsliga sammanslutningar, bokföring, konsumentskydd, utrikeshandeln, handelssjöfart samt farleder för handelssjöfarten, luftfart, kärnkraft, dock så att byggande, innehav och användning av anläggningar för utvinning av kärnkraft eller hantering eller förvaring av material i anslutning härtill får ske i landskapet endast med landskapsregeringens samtycke, standardisering, straffrätt, rättsskipning samt verkställighet av domar och straff, befolkningsskyddet, behörighet att vara verksam inom hälso- och sjukvården, apoteksväsendet, mediciner och produkter av läkemedelstyp, narkotiska ämnen samt framställning av gifter och fastställande av deras användningsändamål, försvarsväsendet och gränsbevakningen, med beaktande av vad

som stadgas i 12 §, ordningsmaktens verksamhet för trygghet av statens säkerhet, försvarstillstånd, beredskap inför undantagsförhållanden, televäsendet, dock så att tillstånd att utöva allmän televerksamhet i landskapet får beviljas av en riksmyndighet endast med landskapsregeringens samtycke, och övriga angelägenheter som enligt grundsatserna i självstyrelselagen ska hänföras till rikets lagstiftningsbehörighet. Enligt 29 § 5 punkten självstyrelselagen har riket även lagstiftningsbehörighet i fråga om bank- och kreditväsendet.

Enligt förarbetena till självstyrelselagen, s. 74 i RP 73/1990 rd, omfattar rikets lagstiftningsbehörighet enligt punkten 8 endast associationsrätten samt lagstiftningen om bokföringen och inte offentlighetsrättsliga sammanslutningar. Enligt förarbetena omfattar vidare rikets behörighet om konsumentskyddet däremot inte lagstiftningsbehörighet i fråga om produktsäkerhet, vilken tillfaller landskapet. Enligt förarbetena, s. 75, motsvarar begreppet luftfarten i sak uttrycket lufttrafiken i den tidigare självstyrelselagen. Enligt förarbetena, s. 76, omfattar rikets lagstiftningsbehörighet enligt punkten 28 inte de behörighetsområden som hänför sig till befolkningsskyddet, så som brand- och räddningsväsendet, hälso- och sjukvården med mera, vilka tillfaller landskapet. Vidare framgår det av förarbetena, s. 77, att rikets lagstiftningsbehörighet enligt punkten 30 inte omfattar rätt att lagstifta om försäljning och förvaring av gifter. Det framgår även att stadgandet om rikets lagstiftningsbehörighet om beredskap inför undantagsförhållanden endast avser att gälla egentlig undantagslagstiftning, som på grund av exceptionella förhållanden kräver ingrepp i medborgarnas allmänna rättigheter eller en genomgripande reglering av näringslivet. Beredskapen för undantagsförhållanden omfattar dock uttryckligen inte reglering av näringslivet vid produktionsstörningar under normala förhållanden. Enligt förarbetena, s. 78, framgår slutligen att rikets lagstiftningsbehörighet enligt 40 punkten med televäsendet ursprungligen avsåg telegraf- och telefonväsendena.

Enligt Högsta domstolens utlåtande, se dess utlåtande av den 9 januari 2004 med diarienummer OH 2003/115, avseende landskapslagen om kontroll av brottslig bakgrund hos personer som ska arbeta med barn, faller reglering av straffregister och utdrag ur dessa inom rikets lagstiftningsbehörighet över straffrätten.

Högsta domstolen har i ett utlåtande, se dess utlåtande av den 23 november 2016 med diarienummer OH2017/8, specifikt avseende en antagen blankettlag om tillämpning på Åland av rikslagen om anmälda organ för vissa produktgrupper, jämte vissa därmed intagna undantag, tagit ställning i ett fall där Ålands lagstiftningsbehörighet över den allmänna näringsrätten enligt 18 § 22 punkten självstyrelselagen ställdes gentemot rikets lagstiftningsbehörighet över televäsendet enligt 27 § 40 § självstyrelselagen. Som ledning för uttolkningen av omfattningen av rikets lagstiftningsbehörighet över televäsendet lades dåvarande informationssamhällsbalkens reglering av allmän televerksamhet och överförings- och sändningstjänster i masskommunikationsnät. I uttalandet bedömdes anmälda organ inom televäsendet falla inom ramen för rikets lagstiftningsbehörighet över televäsendet.

Högsta domstolen har vidare i ett annat utlåtande, se dess utlåtande av den 21 november 2018 med diarienummer OH2019/11, avseende landskapslagen om dataskydd, jämte därmed sammanhängande ändringar, bedömt att lagstiftningsbehörigheten avseende de tvärsäktoriella rättsområdena dataskydd eller behandling av personuppgifter, vilka över lag inte omnämns vid uppdelningen av lagstiftningsbehörigheten mellan Åland och riket i självstyrelselagen, bör bedömas utgående från de rättsområden landskapslagstiftningen kan beröra.

Högsta domstolen har även i ett annat utlåtande, se dess utlåtande av den 31 maj 2017 med diarienummer OH2017/133, avseende en landskapslag om finansiering om främjande av en utbyggnad av bredbandsnät, bedömt att

bredbandsnätet, som är ett av de moderna kommunikationsnäten, i ett annat sammanhang kunde hänföras till rikets lagstiftningsbehörighet över televäsendet. Enligt Högsta domstolen aktualiserade lagstiftningen förhållandet mellan den aktuella lagstiftningen och televerksamheten, eftersom lagstiftningsbehörigheten i fråga om televäsendet tillkommer riket enligt 27 § 40 punkten självstyrelselagen. Högsta domstolen synes därmed inskränka rikets lagstiftningsbehörighet över televäsendet till att endast omfatta televerksamhet. Den ifrågavarande landskapslagstiftningen berörde dock främst byggandet av den fysiska infrastrukturen och som sådan föll den inom ramen för Ålands lagstiftningsbehörighet, vilken konstaterades omfatta lagstiftning om landskapsregeringen och under denna lydande myndigheter och inrättningar, byggnads- och planväsendet, vägar och kanaler, farleder för den lokala sjötrafiken samt näringsverksamhet enligt 18 § 1, 7, 21 och 22 punkterna självstyrelselagen. Högsta domstolen ansåg vidare att Ålands lagstiftningsbehörighet över utbyggnaden av infrastrukturen för bredbandsnätet inte äventyrade de syften som hade skyddats i och med att lagstiftningsbehörigheten i fråga om televäsendet i självstyrelselagen tillföll riket. Enligt samma utlåtande uttalades även att den allmänna eller nationella säkerheten kan kräva viss lagstiftning beträffande nättaktörer och att denna reglering skulle falla under riket lagstiftningsbehörighet för försvarsväsendet, ordningsmaktens verksamhet för tryggnad av statens säkerhet, försvarstillstånd och beredskap inför undantagsförhållanden, enligt 27 § 34 punkten självstyrelselagen.

Högsta domstolen fann vidare i ytterligare ett utlåtande, se dess utlåtande av den 31 maj 2023 med diarienummer KKO-HD/520/2023, avseende landskapslagen om ändring av landskapslagen om tillgängliga webbplatser och mobila applikationer inom landskapsförvaltningen, att behörigheten att lagstifta om tillgängligheten till den offentliga förvaltningens digitala tjänster faller inom ramen för Ålands lagstiftningsbehörighet. Högsta domstolen konstaterade vidare att fastän regleringen på lagnivå enligt kompetensfördelningen hörde till landskapet, ansågs den detaljerade tekniska nivån falla under rikets lagstiftningsbehörighet i frågan om standardisering, enligt 27 § 19 punkten självstyrelselagen. Högsta domstolen konstaterade dock att lagen endast innehöll en genom ett EU-direktiv delegerad normgivningsmakt för landskapsregeringen avseende standardisering och att landskapslagen därmed inte innehöll regler som möjliggjorde standardisering i sig, varför regleringen ansågs falla inom ramen för Ålands lagstiftningsbehörighet.

Bedömningen av huruvida Åland har lagstiftningsbehörighet över reglering av de tvärssektoriella frågorna om cybersäkerhet och samhällskritiska verksamhetsutövers motståndskraft ska därmed bedömas utgående från de rättsområden som lagstiftningen kan beröra. Vidare ska lagstiftningsbehörigheten över övriga angelägenheter, det vill säga andra än de som särskilt har uppräknats i självstyrelselagens behörighetsfördelningsbestämmelser, hänföras till antingen riket eller Åland, baserat på självstyrelselagens grunder.

Åland har i sammanhanget lagstiftningsbehörighet över landskapets offentliga förvaltning såväl som den allmänna näringsrätten inom de i självstyrelselagen särskilt utpekade samt övriga sektorer, vilka inte uttryckligen har tillfallit rikets lagstiftningsbehörighet. Åland har vidare i regel bedömts ha lagstiftningsbehörigheten över byggandet av infrastruktur inom de rättsområden där lagstiftningsbehörigheten för trafiken eller näringsrätten helt eller delvis har tillfallit riket, exempelvis inom televäsendet.

Såväl cybersäkerhetsdirektivet som motståndskraftsdirektivet reglerar skyldigheter i förhållande till cybersäkerhets och driftsäkerhetsaspekter för dels offentlig förvaltning, dels olika typer av verksamhetsutövare inom utpekade kritiska sektorer och dels verksamhetsutövare som tillhandahåller utpekade samhällsviktiga tjänster inom de utpekade kritiska sektorerna. Direktiven ska uttryckligen inte påverka medlemsstaternas ansvar för nationell

säkerhet och undantar offentliga verksamhetsutövare inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, vilket tydliggör att regleringen inte direkt är hänförlig till rättsområdena för nationell säkerhet och försvar.

Landskapsregeringen kan konstatera att direktiven främst syftar att åstadkomma en högre allmän beredskap genom införandet av informationssäkerhetsskyldigheter för offentlig förvaltning och verksamhetsutövare inför produktionsstörningar under normala förhållanden, vilket således enligt landskapsregeringen bör falla inom ramen för Ålands lagstiftningsbehörighet. Landskapsregeringen bedömer vidare att Åland bör anses ha lagstiftningsbehörighet över direktivens reglering av landskapets offentliga förvaltning och samtliga utpekade verksamhetsutövare, vilka verkar inom rättsområden som faller under landskapets lagstiftningsbehörighet, se närmare redogörelse av behörighetsfördelningen för respektive direktiv under avsnitten 4.3 och 4.4 nedan. Lagstiftningsbehörigheten över verksamhetsutövarna inom de så kallade digitala sektorerna tarvar dock särskilda överväganden och ställningstaganden, mot bakgrund av rikets lagstiftningsbehörighet över televäsendet, även benämnd televerksamhet, se den närmare bedömningen under avsnittet 4.2 nedan.

4.2 De digitala sektorerna

Till grund för bedömningen bör inledningsvis en definition av televerksamhet i allmänhet och självstyrelselagens mening i synnerhet konstateras, följt av en genomgång av de i direktiven utpekade digitala kritiska sektorernas verksamhetsutövare och deras tjänster, varvid deras verksamhet definieras utifrån om dessa är teleföretag eller inte. Därpå följer en sammanfattande bedömning av lagstiftningsbehörigheten för respektive kategori av verksamhetsutövare.

4.2.1 Definitionen av televerksamhet

I riket regleras televerksamhet i huvudsak i lagen om elektronisk kommunikation, tidigare benämnd informationssamhällsbalken. I lagens 3 § 27 punkt definieras teleföretag som en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand, det vill säga bedriver allmän televerksamhet.

I lagens 3 § 34 punkt definieras nättjänst som en tjänst som tillhandahålls av ett teleföretag (*nätföretag*) för att ett kommunikationsnät som det äger eller på någon annan grund förfogar över ska kunna användas för överföring och distribution av meddelanden. I lagens 3 § 37 punkt definieras kommunikationstjänst som en tjänst som helt eller huvudsakligen utgörs av överföring av meddelanden i kommunikationsnät samt överförings- och sändningstjänster i masskommunikationsnät och interpersonella kommunikationstjänster. I lagens 3 § 39 punkt definieras kommunikationsnät som ett system som består av sammankopplade ledningar och av anordningar och som är avsett för överföring eller distribution av meddelanden via ledning, med radiovågor, optiskt eller på något annat elektromagnetiskt sätt. Enligt lagens förarbeten, s. 90 i RP 213/2013 rd, ska det vid bedömningen av om det är fråga om en icke-avgränsad användarkrets exempelvis nätets och tjänsternas karaktär, nätets och användarkretsens omfattning samt villkoren för att bli användare beaktas.

I samband med rikets genomförande av kodexdirektivet infördes bland annat ett antal nya definitioner, till följd av direktivets utvidgade tillämpningsområde. I 3 § 11b punkten i lagen om elektronisk kommunikation tillkom definitionen av nummeroberoende interpersonell kommunikationstjänst, vilken definieras som en interpersonell kommunikationstjänst som inte använder ett eller flera nummer i nationella eller internationella

nummerplaner. Enligt förarbetena till den ändrade lagen, s. 177 f. i RP 98/2020 rd, avviker denna typ av kommunikationstjänst från traditionell televerksamhet och aktörerna underställdes därmed inte samma krav som andra teleföretag, exempelvis krav på televerksamhetsanmälan. Enligt s. 178 i förarbetena ansågs vidare inte heller innehållstjänster och allmänna IKT-tjänster tillhöra kategorierna nät- eller kommunikationstjänster, med hänvisning till skäl 17 i kodexdirektivet. Som exempel på innehållstjänster nämns särskilt tjänster som tillhandahålls via telefonnummer eller textmeddelandenummer mot tilläggsavgift, också i sådana fall då de debiteras via telefonräkningen, internetsidors eller diskussionsforums innehåll eller publikationer i sociala medier och likaså videor som tillhandahålls på internet, programutbud på linjär tv, radioprogramutbud, beställ-tv-tjänster eller annat betal-tv-innehåll.

Informations- och kommunikationstekniska tjänster, så kallade IKT-tjänster, inbegriper bland annat innehållstjänster. I artikel 2.13 i Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten) definieras IKT-tjänst som en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem. Det handlar därmed inte om nättjänster och kommunikationstjänster i den bemärkelse som televerksamheten traditionellt anses omfatta. Mot bakgrund av detta har därför reglering av IKT-tjänster inte intagits i lagen om elektronisk kommunikation.

Landskapsregeringen bedömer sammantaget att rättsområdet televäsendet i självstyrelselagens mening, enligt dess 27 § 40 punkt, i huvudsak bör likställas med definitionen av allmän televerksamhet enligt lagen om elektronisk kommunikation. Självstyrelselagens grundsatser ger vidare inte vid handen att lagstiftningsbehörigheten för televäsendet är avsedd att åsyfta annan televerksamhet än allmän sådan. Lagstiftningsbehörigheten över televerksamhet, som inte är allmän, samt verksamhetsutövare som tillhandahåller allmänna IKT-tjänster, inbegripet innehållstjänster, bör därmed enligt landskapsregeringen anses tillfalla Åland.

4.2.2 Digital infrastruktur

I cybersäkerhetsdirektivets bilaga I och motståndskraftsdirektivets bilaga upptas den digitala högkritiska sektorn digital infrastruktur, vilken innefattar följande kategorier av verksamhetsutövare:

- Leverantörer av internetknutpunkter, enligt definitionen i artikel 6.18 i cybersäkerhetsdirektivet. En nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik, som tillhandahåller sammankoppling enbart för autonoma system och som varken kräver att den internettrafik som passerar mellan två deltagande autonoma system ska passera genom ett tredje autonomt system eller ändrar trafiken eller påverkar den på något annat sätt.

- Leverantörer av DNS-tjänster, med undantag för operatörer av rotnamsservrar, enligt definitionen i artikel 6.20 i cybersäkerhetsdirektivet. En entitet som tillhandahåller:

- a) allmänna rekursiva tjänster för att lösa domännamnfrågor till internet-slutanvändare, eller

- b) auktoritativa tjänster för att lösa domännamnfrågor för användning av tredje part, med undantag för rotnamsservrar.

- Registreringsenheter för toppdomäner, eller TLD-registreringsenhet, enligt definitionen i artikel 6.21 i cybersäkerhetsdirektivet. En enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen

och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

- Leverantörer av molntjänster, enligt definitionen i artikel 6.30 i cybersäkerhetsdirektivet. En digital tjänst som 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.

- Tillhandahållare av datacentralstjänster, enligt definitionen i artikel 6.31 i cybersäkerhetsdirektivet. En tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

- Tillhandahållare av nätverk för innehållsleverans, enligt definitionen i artikel 6.32 i cybersäkerhetsdirektivet. 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.

- Tillhandahållare av betrodda tjänster, enligt definitionen i artikel 3.19 i Europaparlamentets och rådets förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. En fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster. Enligt definitionen i artikel 3.16 i samma förordning är en betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av:

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplatser eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplatser eller certifikat med anknytning till dessa tjänster.

Enligt definitionen i artikel 3.20 i samma förordning utgör en kvalificerad tillhandahållare av betrodda tjänster en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorgan enligt förordningen. Enligt definitionen i artikel 3.17 i samma förordning utgör en kvalificerad betrodd tjänst en betrodd tjänst som uppfyller tillämpliga krav i förordningen.

- Tillhandahållare av allmänna elektroniska kommunikationsnät, enligt definitionen i artikel 2.8 i kodexdirektivet. Ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter.

- Tillhandahållare av elektroniska kommunikationstjänster, i den mån deras tjänster är allmänt tillgängliga, i den mening som avses i artikel 2.4 i kodexdirektivet. En tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som omfattar, med undantag av tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller utövande av redaktionellt ansvar över sådant innehåll, följande typer av tjänster:

a)) internetanslutningstjänst enligt definitionen i artikel 2.2 i förordning (EU) 2015/2120 om åtgärder rörande en öppen internetanslutning, vilket

utgör en allmänt tillgänglig elektronisk kommunikationstjänst som erbjuder anslutning till internet, och därigenom möjlighet till anslutning mellan praktiskt taget alla ändpunkter på internet, oberoende av vilken nätteknik och terminalutrustning som används,

b) interpersonell kommunikationstjänst, och

c) tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster och för utsändningstjänster.

Leverantörer av internetknutpunkter, leverantörer av DNS-tjänster, med undantag för operatörer av rotnamnsservrar, registreringsenheter för toppdomäner, tillhandahållare av allmänna elektroniska kommunikationsnät och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, i den mån de är nummerberoende, utgör nätföretag, vilka därmed är teleföretag, i och med att de bedriver allmän televerksamhet. Lagstiftningsbehörigheten över dessa bedöms därmed tillfalla rikets lagstiftningsbehörighet.

Leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, tillhandahållare av betrodda tjänster och tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, i den mån de är nummerberoende, utgör IKT-företag som levererar allmänna IKT-tjänster eller innehållstjänster, vilka därmed inte utgör teleföretag, i och med att de inte bedriver allmän televerksamhet. Lagstiftningsbehörigheten över dessa bedöms därmed tillfalla Ålands lagstiftningsbehörighet.

4.2.3 Förvaltning av IKT-tjänster (mellan företag)

I cybersäkerhetsdirektivets bilaga I upptas den digitala högkritiska sektorn Förvaltning av IKT-tjänster (mellan företag), vilken innefattar följande kategorier av verksamhetsutövare:

- Leverantörer av utlokaliserade driftstjänster, enligt definitionen i artikel 6.39 i cybersäkerhetsdirektivet. En verksamhetsutövare som tillhandahåller tjänster som 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.

- Leverantörer av utlokaliserade säkerhetstjänster, enligt definitionen i artikel 6.40 i cybersäkerhetsdirektivet. En leverantör av utlokaliserade driftstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

Leverantörer av utlokaliserade driftstjänster och säkerhetstjänster utgör IKT-företag som levererar IKT-tjänster, det vill säga installations-, förvaltnings-, drifts- eller underhållstjänster, vilka därmed inte utgör teleföretag, i och med att de inte bedriver allmän televerksamhet. Lagstiftningsbehörigheten över dessa bedöms därmed tillfalla Ålands lagstiftningsbehörighet.

4.2.4 Digitala leverantörer

I cybersäkerhetsdirektivets bilaga II uppräknas den digitala andra kritiska sektorn Digitala leverantörer, vilken innefattar följande kategorier av verksamhetsutövare:

- Leverantörer av marknadsplatser online, enligt definitionen i artikel 6.28 i cybersäkerhetsdirektivet, vilket utgör en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenterna på den inre marknaden. En tjänst som använder programvara, inbegripet en webbplats, en del av en webbplats eller en applikation, som administreras av en näringsidkare eller för dennas räkning, som ger

konsumenterna möjlighet att ingå distansavtal med andra näringsidkare eller konsumenter.

- Leverantörer av sökmotorer, enligt definitionen i artikel 6.29 i cybersäkerhetsdirektivet, vilket utgör en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150. En digital tjänst som gör det möjligt för användare att mata in sökfraser för att göra sökningar på i princip alla webbplatser eller alla webbplatser på ett visst språk på grundval av en fråga om vilket ämne som helst i form av ett nyckelord, en röstbegäran, en fras eller någon annan inmatning och som returnerar resultat i vilket format som helst som innehåller information om det begärda innehållet.

- Leverantörer av plattformar för sociala nätverkstjänster, enligt definitionen i artikel 6.33 i cybersäkerhetsdirektivet. En plattform som 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.

Leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster utgör IKT-företag som levererar allmänna IKT-tjänster eller innehållstjänster, vilka därmed inte utgör teleföretag, i och med att de inte bedriver allmän televerksamhet. Lagstiftningsbehörigheten över dessa bedöms därmed tillfalla Ålands lagstiftningsbehörighet.

4.3 Cybersäkerhetsdirektivet

Cybersäkerhetsdirektivets tillämpningsområde omfattar 18 olika sektorer, med delsektorer och typer av verksamhetsutövare, varav offentlig förvaltning utgör en. Cybersäkerhetsdirektivets reglering tar i huvudsak sikte på beredskap under normala förhållanden, vilket tydliggörs av undantagen för nationell säkerhet. Åland har därmed inom landskapet, mot bakgrund av genomgången ovan, lagstiftningsbehörighet inom merparten av de sektorer och rättsområden som direktivets reglering omfattar, med följande undantag, vilka tillhör rikets lagstiftningsbehörighet:

Högkритiska sektorer:

- Bankverksamhet, enligt 29 § 5 punkten självstyrelselagen.

- Finansmarknadsinfrastruktur, enligt 29 § 5 punkten självstyrelselagen.

Högkritiska verksamhetsutövartyper:

- Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 som bedriver leverans enligt definitionen i artikel 2.12 i det direktivet, till delen de begagnar sig av kärnkraft, enligt 27 § 18 § självstyrelselagen.

- Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944, till delen de begagnar sig av kärnkraft, enligt 27 § 18 § självstyrelselagen.

- Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften, enligt 27 § 14 punkten självstyrelselagen.

- Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004, enligt 27 § 14 punkten självstyrelselagen.

- Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004, exklusive de enskilda fartyg som drivs av dessa företag, till delen de bedriver handelssjöfart samt verksamheten berör farleder för handelssjöfarten, enligt 27 § 13 punkten självstyrelselagen, med begränsningarna enligt 18 § 21 punkten.

- Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG, till delen de

bedriver handelssjöfart samt verksamheten berör farleder för handelssjöfarten, enligt 27 § 13 punkten självstyrelselagen, med begräsningarna enligt 18 § 21 punkten.

- Verksamhetsutövare som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG, enligt 27 § 30 punkten självstyrelselagen.

- Verksamhetsutövare som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2, enligt 27 § 30 punkten självstyrelselagen.

- Verksamhetsutövare som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123, enligt 27 § 30 punkten självstyrelselagen.

- Leverantörer av internetknutpunkter, enligt 27 § 40 punkten självstyrelselagen.

- Leverantörer av DNS-tjänster, med undantag för operatörer av rot-namnservrar, enligt 27 § 40 punkten självstyrelselagen.

- Registreringsenheter för toppdomäner, enligt 27 § 40 punkten självstyrelselagen.

- Tillhandahållare av allmänna elektroniska kommunikationsnät, enligt 27 § 40 punkten självstyrelselagen.

- Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, i den mån de är nummerberoende, enligt 27 § 40 punkten självstyrelselagen.

Andra kritiska sektorer:

- Tillverkning, produktion och distribution av kemikalier, till delen tillverkning och produktion, enligt 27 § 30 punkten självstyrelselagen.

- Forskning, till den del som denna inte är hänförlig till rättsområden inom landskapets lagstiftningsbehörighet, enligt 27 § självstyrelselagen.

Till den del som cybersäkerhetsdirektivet reglerar verksamhetsutövare inom enskilda sektorer särskilt faller dessa stadganden därmed även inom ramen för rikets respektive landskapets lagstiftningsbehörighet över respektive sektor.

Till de delar som cybersäkerhetsdirektivet förutsätter kommunikation mellan den behöriga myndigheten, cyberkrishanteringsmyndigheten och enheten för hantering av cybersäkerhetsincidenter och kommissionen eller andra organ, myndigheter och samarbetsgrupper inom den Europeiska unionen samt andra medlemsstaters behöriga myndigheter eller enheter måste denna ske genom rikets gemensamma kontaktpunkt, till följd av rikets lagstiftningsbehörighet över förhållandet till utländska makter enligt 27 § 4 punkten självstyrelselagen.

Till detta kommer vidare att riket har lagstiftningsbehörigheten över de delar av cybersäkerhetsdirektivet vilka föreskriver införandet av en nationell strategi, en gemensam kontaktpunkt, en samordnande cyberkrishanteringsmyndighet, en samordnande enhet för hantering av cybersäkerhetsincidenter och en förteckning över identifierade verksamhetsutövare enligt 59b § 2 och 3 mom. självstyrelselagen.

Cybersäkerhetsdirektivets övriga stadganden torde dock falla inom ramen för landskapets lagstiftningsbehörighet.

4.4 Motståndskraftsdirektivet

Motståndskraftsdirektivets tillämpningsområde omfattar 11 olika sektorer, med undersektorer och kategorier av verksamhetsutövare, varav offentlig förvaltning utgör en. Motståndskraftsdirektivets reglering tar i huvudsak sikte på beredskap under normala förhållanden, vilket tydliggörs av

undantagen för nationell säkerhet. Åland har därmed inom landskapet, mot bakgrund av genomgången ovan, lagstiftningsbehörighet inom merparten av de sektorer och rättsområden som direktivets reglering omfattar, med följande undantag, vilka tillhör rikets lagstiftningsbehörighet:

Kritiska sektorer:

- Bankverksamhet, enligt 29 § 5 punkten självstyrelselagen.
- Finansmarknadsinfrastruktur, enligt 29 § 5 punkten självstyrelselagen.

Kritiska verksamhetsutövarkategorier:

- Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 som bedriver leverans enligt definitionen i artikel 2.12 i det direktivet, till delen de begagnar sig av kärnkraft, enligt 27 § 18 § självstyrelselagen.

- Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944, till delen de begagnar sig av kärnkraft, enligt 27 § 18 § självstyrelselagen.

- Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften, enligt 27 § 14 punkten självstyrelselagen.

- Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004, enligt 27 § 14 punkten självstyrelselagen.

- Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004, exklusive de enskilda fartyg som drivs av dessa företag, till delen de bedriver handelssjöfart samt verksamheten berör farleder för handelssjöfarten, enligt 27 § 13 punkten självstyrelselagen, med begränsningarna enligt 18 § 21 punkten.

- Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG, till delen de bedriver handelssjöfart samt verksamheten berör farleder för handelssjöfarten, enligt 27 § 13 punkten självstyrelselagen, med begränsningarna enligt 18 § 21 punkten.

- Leverantörer av internetknutpunkter, enligt 27 § 40 punkten självstyrelselagen.

- Leverantörer av DNS-tjänster, med undantag för operatörer av rot-namnsservrar, enligt 27 § 40 punkten självstyrelselagen.

- Registreringsenheter för toppdomäner, enligt 27 § 40 punkten självstyrelselagen.

- Tillhandahållare av allmänna elektroniska kommunikationsnät, enligt 27 § 40 punkten självstyrelselagen.

- Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, i den mån de är nummerberoende, enligt 27 § 40 punkten självstyrelselagen.

Till den del som motståndskraftsdirektivet reglerar verksamhetsutövare inom enskilda sektorer särskilt faller dessa stadganden därmed även inom ramen för rikets respektive landskapets lagstiftningsbehörighet över respektive sektor.

Till de delar som motståndskraftsdirektivet förutsätter kommunikation mellan den behöriga myndigheten och kommissionen eller andra organ, myndigheter och samarbetsgrupper inom den Europeiska unionen samt andra medlemsstaters behöriga myndigheter eller enheter måste denna ske genom rikets gemensamma kontaktpunkt, till följd av rikets lagstiftningsbehörighet över förhållandet till utländska makter enligt 27 § 4 punkten självstyrelselagen.

Därutöver faller även enskilda stadganden, i helhet eller till delar, inom ramen för rikets lagstiftningsbehörighet. Det handlar bland annat om

straffregisterkontroll enligt artikel 14.3 i motståndskraftsdirektivet, vilken bör anses falla inom rättsområdet straffrätten, vilken omfattas av rikets lagstiftningsbehörighet enligt 27 § 22 punkten i självstyrelselagen. I aktuellt fall innehåller landskapets genomförande därför enbart en informativ hänvisning till rikslagstiftningen på detta område.

Till detta kommer vidare att riket har lagstiftningsbehörigheten över de delar av motståndskraftsdirektivet vilka föreskriver införandet av en nationell strategi, en nationell riskbedömning, en gemensam kontaktpunkt och en förteckning över identifierade verksamhetsutövare enligt 59b § 2 och 3 mom. självstyrelselagen.

Motståndskraftsdirektivets övriga stadganden torde dock falla inom ramen för landskapets lagstiftningsbehörighet.

5. Förslagets verkningar

5.1 Allmänt

Lagförslaget kan förväntas leda till en ökad nivå av cybersäkerhet och motståndskraft hos berörda offentliga och enskilda verksamhetsutövare samt därigenom i landskapet i stort. Lagförslaget kan vidare, tillsammans med övriga nationella genomföranden, förväntas leda till att relevanta myndigheter i högre grad samordnar och samarbetar inom cybersäkerhet och motståndskraft på såväl åländsk som nationell och internationell nivå, jämte därmed sammanhängande ökat kunskaps- och erfarenhetsutbyte. Lagförslaget förväntas även leda till en höjd säkerhet avseende hanteringen av personuppgifter och minska risken för personuppgiftsincidenter hos berörda verksamhetsutövare, med hänvisning till att en förhöjd teknisk cybersäkerhetsnivå kan förväntas leda till en snabbare upptäckt av personuppgiftsincidenter, ett starkare inbyggt dataskydd och dataskydd som standard.

Lagförslaget innebär vidare att nya uppgifter och skyldigheter påförs såväl myndigheter som offentliga och enskilda verksamhetsutövare, vilket förväntas leda till ökad administration och mer eller mindre omfattande strukturella förändringsarbeten hos enskilda verksamhetsutövare, vilka i sin tur förutsätter ytterligare resurstilldelning och kompetenstillskott.

Lagförslaget förväntas samtidigt leda till att de samlade samhällskostnaderna för negativa konsekvenser av cybersäkerhets- eller andra incidenter hos verksamhetsutövare minskar.

Tillämpningsområdet för lagen kommer åtminstone att omfatta landskapsregeringens underlydande myndigheter, i egenskap av att de definieras som offentliga verksamhetsutövare. Inom landskapet återfinns därutöver ungefär 40 medelstora och stora företag enligt kommissionens definition vilka därtill är verksamma inom ramen för uppräknade sektorer i cybersäkerhetsdirektivets bilagor. Dessa enskilda verksamhetsutövare kommer därmed att klassificeras som antingen väsentliga eller viktiga verksamhetsutövare och därmed omfattas av antingen rikets eller landskapets cybersäkerhetsdirektivs genomförande, beroende på lagstiftningsbehörigheten. Den absolut största delen av dessa bedöms dock falla under landskapets lagstiftningsbehörighet. Till detta kan även andra landskaps- eller kommunala myndigheter samt offentliga som enskilda verksamhetsutövare tillkomma, oavsett storlek, genom att de av landskapsregeringen identifieras som kritiska, väsentliga eller viktiga verksamhetsutövare. Detta främst till följd av deras bedömt europeiska, nationella, regionala eller sektoriella betydelse och därmed potentiella negativa betydande störande effekt eller påverkan på upprätthållandet av kritisk samhällelig eller ekonomisk verksamhet, andra samhällsviktiga tjänster, andra verksamhetsutövare, andra medlemsstater eller viktiga samhällsintressen.

5.2 Ekonomiska verkningar

Lagförslaget kan förväntas leda till ökade ekonomiska kostnader för berörda verksamhetsutövare, till följd av lagens krav på utbildning, riskhanteringsåtgärder och rapporteringsskyldigheter.

Det är på förhand nära nog omöjligt att uppskatta hur många verksamhetsutövare på Åland som kommer att omfattas av regleringen och i vilken mån dessa behöver vidta ytterligare riskhanteringsåtgärder för ökad cybersäkerhet och motståndskraft i förhållande till dagsläget.

Lagförslagets införande av rapporteringsskyldighet vid incidenter och krav på informationsutbyten kan dock förväntas leda till en ökad administration, i den mån som en verksamhetsutövare är föremål för cybersäkerhets- eller andra incidenter. Vidare kan landskapsregeringens tillsyn förväntas leda till ökade kostnader för landskapsregeringen, jämte ett visst kostnadsdrivande merarbete för tillsynade verksamhetsutövare.

Klart står därmed att lagförslaget innebär ökade kostnader för berörda verksamhetsutövare, emedan storleken på dessa kan komma att variera kraftigt beroende på sektor och till vilken grad visst arbete sker redan idag sker vid en viss verksamhetsutövare.

En viktig verksamhetsutövare kan inom ramen för sitt ålagda cybersäkerhetsarbete förväntas åtminstone ha ett grundläggande skydd på plats, bestående av brandväggar, antiviruskydd, skydd för enheter samt processer för incidenthantering, driftskontinuitet och krishantering. För väsentliga verksamhetsutövare kan vidare säkerhetsövervakning samt egna återkommande säkerhetsrevisioner och penetrationstester förväntas tillkomma. Beroende på riskanalysen, storleken och huruvida verksamhetsutövaren är viktig eller väsentlig kan årliga kostnader för åtgärder för cybersäkerhet för en genomsnittlig berörd verksamhetsutövare förväntas ligga på ungefär 30 000–100 000 euro per år.

Samtidigt förväntas lagförslaget leda till minskade negativa ekonomiska konsekvenser till följd av cybersäkerhets- eller andra incidenter hos verksamhetsutövare, såväl för samhället i stort som för verksamhetsutövarna själva och andra verksamhetsutövare, myndigheter eller enskilda vilka nyttjar deras produkter eller tjänster.

Landskapsregeringen förväntas i samband med genomförandets ikraftträdande och dess identifiering av kritiska, väsentliga och viktiga verksamhetsutövare genomföra en mer utförlig och konkret analys av vilka verksamhetsutövare som omfattas och den aktuella lägesbilden avseende deras cybersäkerhets- och motståndskraftsarbete.

5.3 Verkningar för myndigheterna

Landskapsregeringen kommer, i egenskap av tillsynsmyndighet, cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter, att behöva tillföras ytterligare kompetens och resurstillskott. De uppgifter som landskapsregeringen påförs kräver en bred specialistkompetens inom områdena cybersäkerhet, motståndskraft och allmän säkerhet. Därutöver tillkommer behovet av ändamålsenliga arbetsmetoder, arbetsverktyg och utrustning samt tekniska hjälpmedel för såväl den löpande skötseln av myndighetens uppgifter som dess tillsynsuppdrag.

I dagsläget återfinns landskapsregeringens kompetens inom cybersäkerhet vid landskapsregeringens digitaliseringsenhet, men särskilt utpekade personalresurser och nödvändiga programvaror för de i lagförslaget tillkommande myndighetsuppgifterna saknas till stora delar till följd av att enheten idag saknar myndighetsuppgifter. Landskapsregeringens kompetens inom motståndskraft och allmän säkerhet är vidare bristfällig och på intet sätt heltäckande samt återfinns främst hos enskilda tjänstemän vid Regeringskansliet och Infrastrukturavdelningen. Lagförslagets praktiska

genomförande förutsätter därmed att landskapsregeringen tillförs resurser i form av nya årsverken och ekonomiska medel för främst upphandling av nya arbetsverktyg, licenser till dessa och utbildning.

Landskapsregeringens digitaliseringsenhet förväntas genom lagstiftningen påföras uppgifter motsvarande åtminstone två nya årsverken över tid, ett för lösandet av landskapsregeringens uppgifter i egenskap av enhet för hantering av cybersäkerhetsincidenter och cyberkrishanteringsmyndighet och ett för lösandet av landskapsregeringens övriga tillsynsuppgifter och administration. Den årliga kostnaden för de två årsverkerna per beräknas utifrån 2024 års löneklasser till ett maximalt totalbelopp om ungefär 170 000 euro per år. Därtill förväntas digitaliseringsenheten få ökade utgifter om ungefär 60 000 euro för upphandling av nya arbetsverktyg och licenser till dessa till följd av landskapsregeringens ålagda myndighetsuppdrag samt ungefär 60 000 euro för framtagandet av nya arbetsrutiner och arbetsprocesser samt dokumentation av dessa för landskapsregeringens eget cybersäkerhetsarbete. Dessa totala uppskattade kostnadsökningar om ungefär 290 000 euro under det första året, följda av en årlig kostnad om ungefär 170 000 euro, bedöms kunna hanteras inom ramen för Digitaliseringsenhetens nuvarande budget, förutsatt att några sänkningar av denna inte sker under kommande år.

Landskapsregeringen förväntas vidare påföras kostnadsökningar motsvarande åtminstone ett årsverke över tid, förslagsvis vid landskapsregeringens regeringskansli, för lösandet av landskapsregeringens tillsynsuppgifter till följd av genomförandet av motståndskraftdirektivet med motståndskraft och allmän säkerhet som huvuduppgift, uppgående till en årlig kostnad om ungefär 80 000 euro per år. Den nya tjänsten skulle även kunna fungera som samordnare av landskapsregeringens redan förekommande och i dagsläget uppdelade säkerhets- och beredskapsarbete. Regeringskansliet kan till följd av detta förväntas drabbas av kostnadsökningar om ungefär 30 000 euro per år för nödvändig upphandling av utbildning samt nya arbetsverktyg och teknisk utrustning, vilket medför totala kostnadsökningar för Regeringskansliet om ungefär 110 000 euro per år.

Landskapsregeringen har för närvarande ingen tjänsteman i beredskap eller annan typ av jour eller beredskap för att hantera oförutsedda händelser, incidenter eller allvarliga störningar vilka inträffar efter ordinarie arbetstid. Dessutom saknas en samordningspunkt för landskapsregeringens krisledning, varvid en tjänsteman fungerar som central kontaktyta för andra aktörer vid oförutsedda händelser, incidenter eller allvarliga störningar inom landskapsregeringens verksamhetsområden. Beredskap och behov kan samordnas inom ramen för landskapsregeringen, men det krävs att varje förvaltning och verksamhetsområde har förmåga att verkställa sina beredskapsåtgärder inom ramen för ett systematiskt arbetssätt. För att upprätthålla en sådan beredskap över tid bedöms ungefär fem årsverken behövas, vilket i dagsläget inte finns på plats eller har planerats för. För det fall att något sådant inte införs kan landskapet nödgas ingå en överenskommelseförordning med riket om skötandet av exempelvis uppgifterna rörande stöd vid incidenthanteringen och incidentrapporteringen vilka åläggs enheten för hantering av cybersäkerhetsincidenter på tider och dagar utanför ordinarie arbetstider och dagar som inte är helgdagar. En överenskommelseförordning innebär dock att landskapet åläggs en avgift motsvarande kostnaden för den tjänst vilken en av rikets myndigheter tillhandahåller till landskapet.

Landskapsregeringens underlydande myndigheter, samt i förekommande fall enskilda kommuner och kommunala myndigheter, kan vidare, i egenskap av att de uppfyller kraven för att klassificeras eller identifieras som kritiska, väsentliga eller viktiga verksamhetsutövare, förväntas drabbas av samma verkningar som övriga enskilda verksamhetsutövare till följd av lagens kravställning.

5.4 Övriga samhällliga verkningar

Lagförslaget kan förväntas leda till att samhällskostnaderna vilka orsakas av negativa effekter av incidenter och cybersäkerhetsincidenter minskar, till följd av att det åländska samhället i stort får en förhöjd cybersäkerhets- och motståndskraftsnivå.

En ökad motståndskraft och säkerhet för kritiska verksamhetsutövare kan vidare förväntas minska risken för miljöskador och utsläpp vid dessa.

Lagförslaget förväntas inte innebära några särskilda konsekvenser för jämställdheten mellan könen.

6. Ärendets beredning

Landskapsregeringen beslutade den 30 januari 2024 att överföra en lagstiftningspromemoria om genomförande av cybersäkerhetsdirektivet på Åland till lagberedningen för lagstiftningsåtgärder.

Landskapsregeringen beslutade den 28 mars 2024 att överföra en lagstiftningspromemoria om genomförande av motståndskraftsdirektivet på Åland till lagberedningen för lagstiftningsåtgärder.

Lagförslaget har beretts som tjänstemannaberedning vid lagberedningen, i samråd med relevanta sakkunniga inom landskapsregeringen och andra intressenter.

Lagförslaget har utsänts på remiss till 35 remissinstanser: Regeringskansliet, Finansavdelningen, Social- och miljöavdelningen, Utbildnings- och kulturavdelningen, Näringsavdelningen, Infrastrukturavdelningen, Ålands landskapsarkiv, Ålands miljö- och hälsoskyddsmyndighet, Ålands arbetsmarknads- och studieservicemyndighet, Ålands hälso- och sjukvård, Ålands ombudsmannamyndighet, Datainspektionen, Ålands statistik- och utredningsbyrå, Landskapets fastighetsverk, Fordonsmyndigheten, Ålands kulturdelegation, Ålands energimyndighet, Ålands gymnasium, Högskolan på Åland, Ålands folkhögskola, Ålands musikinstitut, Landskapet Ålands pensionsfond, Ålands sjösäkerhetscentrum, Ålands kommunförbund, Oasen boende- och vårdcenter, Kommunernas socialtjänst kommunalförbund, Kommunalförbundet för Ålands Miljöservice, Mariehamns stad, Jomala kommun, Ålands näringsliv, Företagarna på Åland, Inrikesministeriet, Transport- och kommunikationsverket, Dataombudsmannens byrå och Försörjningsberedskapscentralen.

Lagförslaget har även i samband med remissutskicket utsänts för känedom till landskapets övriga 14 kommuner.

+ av remissinstanserna avgav + utlåtanden, vilka har beaktats i det fortsatta lagberedningsarbetet. Remissinstanserna har över lag + eller ställt sig + till lagförslaget.

Detaljmotivering

Landskapslag om cybersäkerhet och motståndskraft

1 kap. Allmänna bestämmelser

1 §. *Lagens syfte.* I denna paragraf föreskrivs om lagens syfte.

Enligt paragrafens 1 punkt är ett av lagens syften att uppnå en hög cybersäkerhetsnivå. Bestämmelsen genomför art. 1.1 i cybersäkerhetsdirektivet.

Enligt paragrafens 2 punkt anges lagens syfte att uppnå en hög grad av motståndskraft och säkerställa tillhandahållandet av samhällsviktiga tjänster. Bestämmelsen genomför art. 1.1 led e i motståndskraftsdirektivet.

2 §. *Definitioner.* I denna paragraf definieras de viktigaste begreppen som används i lagen, vilka enbart genomförs till den del som de är av betydelse

för reglering av verksamhetsutövare som faller inom ramen för Ålands lagstiftningsbehörighet.

I paragrafens *1 punkt* definieras cybersäkerhetsdirektivet som 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).

I paragrafens *2 punkt* definieras motståndskraftsdirektivet som Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

I paragrafens *3 punkt* definieras den allmänna dataskyddsförordningen som 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).

I paragrafens *4 punkt* definieras nätverks- och informationssystem som ett elektroniskt kommunikationsnät, en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av punkterna a och b för att de ska kunna drivas, användas, skyddas och underhållas. Bestämmelsen genomför definitionen av nätverks- och informationssystem i art. 6.1 i cybersäkerhetsdirektivet, vari definitionen av elektroniskt kommunikationsnät kopplas till definitionen i art. 2.1 i kodexdirektivet. Elektroniska kommunikationsnät ska i sammanhanget inte sammankopplas med de så kallade allmänna elektroniska kommunikationsnäten, utan avser i sammanhanget de nätverks- och informationssystem som verksamhetsutövare som verkar inom ramen för åländsk lagstiftningsbehörighet tillhandahåller eller begagnar sig av när de tillhandahåller tjänster.

I paragrafens *5 punkt* definieras säkerhet i nätverks- och informationssystem som nätverks- och informationssystemets förmåga att med en viss tillförlitlighetsnivå motså händelser som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem. Bestämmelsen genomför definitionen av säkerhet i nätverks- och informationssystem i art. 6.2 i cybersäkerhetsdirektivet.

I paragrafens *6 punkt* definieras cybersäkerhet enligt definitionen i art. 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). Bestämmelsen genomför definitionen av cybersäkerhet i art. 6.3 i cybersäkerhetsdirektivet.

I paragrafens *7 punkt* definieras tillbud som en händelse vilken kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod. Bestämmelsen genomför definitionen av tillbud i art. 6.5 i cybersäkerhetsdirektivet.

I paragrafens *8 punkt* definieras cybersäkerhetsincident som en händelse vilken undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Bestämmelsen genomför definitionen av cybersäkerhetsincident i art. 6.6 i cybersäkerhetsdirektivet.

I paragrafens *9 punkt* definieras storskalig cybersäkerhetsincident som en cybersäkerhetsincident vilken orsakar störningar som är så omfattande att Finland inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater i Europeiska unionen. Bestämmelsen genomför definitionen av storskalig cybersäkerhetsincident i art. 6.7 i cybersäkerhetsdirektivet.

I paragrafens *10 punkt* definieras incident som varje händelse vilken kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst, inbegripet när den påverkar de nationella system som skyddar rättsstatens principer. Bestämmelsen genomför definitionen av incident i art. 2.3 i motståndskraftsdirektivet.

I paragrafens *11 punkt* definieras incidenthantering som alla åtgärder och förfaranden vilka syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident. Bestämmelsen genomför definitionen av incidenthantering i art. 6.8 i cybersäkerhetsdirektivet.

I paragrafens *12 punkt* definieras risk som risk för förlust eller störning orsakad av en incident, vilken ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar. Bestämmelsen genomför definitionen av risk i art. 6.9 i cybersäkerhetsdirektivet jämte art. 2.6 i motståndskraftsdirektivet.

I paragrafens *13 punkt* definieras riskbedömning som den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror som 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. Bestämmelsen genomför definitionen av riskbedömning i art. 2.7 i motståndskraftsdirektivet.

I paragrafens *14 punkt* definieras cyberhot som ett cyberhot enligt definitionen i art. 2.8 i cybersäkerhetsakten, vilken avser en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer. Bestämmelsen genomför definitionen av cyberhot i art. 6.10 i cybersäkerhetsdirektivet.

I paragrafens *15 punkt* definieras betydande cyberhot som ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövers nätverks- och informationssystem eller användarna av verksamhetsutövers tjänster genom att vålla betydande materiell eller immateriell skada. Bestämmelsen genomför definitionen av betydande cyberhot i art. 6.11 i cybersäkerhetsdirektivet.

I paragrafens *16 punkt* definieras IKT-produkt som en IKT-produkt enligt definitionen i art. 2.12 i cybersäkerhetsakten, vilken avser en del, eller en grupp av delar, i nätverks- och informationssystem. IKT utgör en förkortning för de vedertagna tekniska begreppen informations- och kommunikationsteknik eller informations- och kommunikationsteknisk. Bestämmelsen genomför definitionen av IKT-produkt i art. 6.12 i cybersäkerhetsdirektivet.

I paragrafens *17 punkt* definieras IKT-tjänst som en IKT-tjänst enligt definitionen i art. 2.13 i cybersäkerhetsakten, vilken avser en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem. Bestämmelsen genomför definitionen av IKT-tjänst i art. 6.13 i cybersäkerhetsdirektivet.

I paragrafens *18 punkt* definieras IKT-process som en IKT-process enligt definitionen i art. 2.14 i cybersäkerhetsakten, vilken avser verksamhet som utförs för att utforma, utveckla, tillhandahålla eller underhålla en IKT-produkt eller IKT-tjänst. Bestämmelsen genomför definitionen av IKT-process i art. 6.14 i cybersäkerhetsdirektivet.

I paragrafens *19 punkt* definieras sårbarhet som en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett

cyberhot. Bestämmelsen genomför definitionen av sårbarhet i art. 6.15 i cybersäkerhetsdirektivet.

I paragrafens 20 punkt definieras standard som en standard enligt definitionen i art. 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 (nedan kallad *standardiseringsförordningen*). Enligt standardiseringsförordningen avser en standard en teknisk specifikation som antagits av ett erkänt standardiseringsorgan för upprepad eller fortlöpande tillämpning, som inte är tvingande och som tillhör någon av följande typer:

a) internationell standard: en standard som antagits av ett internationellt standardiseringsorgan,

b) europeisk standard: en standard som antagits av en europeisk standardiseringsorganisation,

c) harmoniserad standard: en europeisk standard som antagits på grundval av kommissionens begäran för tillämpningen av unionens harmoniseringslagstiftning, eller

d) nationell standard: en standard som antagits av ett nationellt standardiseringsorgan.

Bestämmelsen genomför definitionen av standard i art. 6.16 i cybersäkerhetsdirektivet jämte art. 2.8 i motståndskraftsdirektivet.

I paragrafens 21 punkt definieras teknisk specifikation som en teknisk specifikation enligt definitionen i art. 2.4 i standardiseringsförordningen, vilken avser ett dokument som föreskriver de tekniska krav som en produkt, process, tjänst eller ett system ska uppfylla och som fastställer ett eller flera av följande:

a) De egenskaper som krävs av en produkt, exempelvis i fråga om kvalitetsnivåer, prestanda, interoperabilitet, miljöskydd, hälsa, säkerhet eller dimensioner, och inbegripet sådana krav som avser varubeteckning, terminologi, symboler, provning och provningsmetoder, förpackning, märkning eller etikettering samt förfaranden för bedömning av överensstämmelse.

b) Produktionsmetoder och processer för de jordbruksprodukter som definieras i artikel 38.1 i EUF-fördraget, för produkter avsedda att konsumeras av människor eller djur samt läkemedel, liksom produktionsmetoder och processer för andra produkter om de påverkar dessa produkters egenskaper.

c) De krav som ställs på en tjänst, inklusive kvalitetsnivåer, prestanda, interoperabilitet, miljöskydd, hälsa eller säkerhet, och inbegripet krav på leverantören om att ställa uppgifter till tjänstemottagarnas förfogande i enlighet med artikel 22.1–22.3 i Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden.

d) Metoder och kriterier för bedömning av byggprodukters prestanda enligt artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 305/2011 om fastställande av harmoniserade villkor för saluföring av byggprodukter, i förhållande till deras väsentliga egenskaper.

Bestämmelsen genomför definitionen av teknisk specifikation i art. 6.17 i cybersäkerhetsdirektivet jämte art. 2.9 i motståndskraftsdirektivet.

I paragrafens 22 punkt definieras digital tjänst som alla informationssamhällets tjänster, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. Definitionen är kopplad till definitionen en tjänst enligt definitionen i art. 1.1 led b i Europaparlamentets och rådets direktiv (EU) 2015/1535 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (nedan kallad *anmälningsdirektivet*). Med på distans avses definitionen av detta i art. 1.1 led b mom. 2 led i

i anmälningsdirektivet, vilket definieras som en tjänst som tillhandahålls utan att parterna är närvarande samtidigt. Med på elektronisk väg avses definitionen av på distans i art. 1.1 led b mom. 2 led ii i anmälningsdirektivet, vilket definieras som en tjänst som sänds vid utgångspunkten och tas emot vid slutpunkten med hjälp av utrustning för elektronisk behandling, inbegripet digital signalkomprimering, och lagring av uppgifter, och som i sin helhet sänds, befordras och tas emot genom tråd, radio, optiska medel eller andra elektromagnetiska medel. Med på individuell begäran av en tjänstemottagare avses definitionen av detta i art. 1.1 led b mom. 2 led iii i anmälningsdirektivet, vilket definieras som en tjänst som tillhandahålls genom överföring av uppgifter på individuell begäran. I bilaga I till anmälningsdirektivet återfinns en vägledande förteckning över tjänster som inte omfattas av definitionerna i art. 1.1 led b mom. 2. Bestämmelsen genomför definitionen av digital tjänst i art. 6.23 i cybersäkerhetsdirektivet.

I paragrafens 23 *punkt* definieras betrodd tjänst som en betrodd tjänst enligt definitionen i art. 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 (nedan kallad *förordningen om elektronisk identifiering*). Enligt förordningen om elektronisk identifiering avses med betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av:

a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplatser eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

c) bevarande av elektroniska underskrifter, stämplatser eller certifikat med anknytning till dessa tjänster.

Bestämmelsen genomför definitionen av betrodd tjänst i art. 6.24 i cybersäkerhetsdirektivet.

I paragrafens 24 *punkt* definieras tillhandahållare av betrodda tjänster som en tillhandahållare av betrodda tjänster enligt definitionen i art. 3.19 i förordningen om elektronisk identifiering, vilken avser en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster. Bestämmelsen genomför definitionen av tillhandahållare av betrodda tjänster i art. 6.25 i cybersäkerhetsdirektivet.

I paragrafens 25 *punkt* definieras kvalificerad betrodd tjänst: en kvalificerad betrodd tjänst enligt definitionen i art. 3.17 i förordningen om elektronisk identifiering, en betrodd tjänst som uppfyller tillämpliga krav i förordningen. Bestämmelsen genomför definitionen av kvalificerat betrodd tjänst i art. 6.26 i cybersäkerhetsdirektivet.

I paragrafens 26 *punkt* definieras kvalificerad tillhandahållare av betrodda tjänster som en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i art. 3.20 i förordningen om elektronisk identifiering, vilken avser en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet. Bestämmelsen genomför definitionen av kvalificerad tillhandahållare av betrodda tjänster i art. 6.27 i cybersäkerhetsdirektivet.

I paragrafens 27 *punkt* definieras internetbaserad marknadsplats: en i 6 kap. 8 § 4 punkten i konsumentskyddslagen (FFS 38/1978) avsedd internetbaserad marknadsplats, vilken avser en tjänst som erbjuder konsumenten möjlighet att ingå distansavtal med andra näringsidkare än den som tillhandahåller marknadsplatsen eller med privatpersoner och som utnyttjar den webbplats, applikation eller annat program eller en del av det som används

av den som tillhandahåller marknadsplatsen eller på dennes vägnar. Rikets bestämmelse är i sin tur ett genomförande av definitionen av en marknadsplats online enligt definitionen i art. 2 led n i Europaparlamentets och rådets direktiv 2005/29/EG om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder). Bestämmelsen genomför definitionen av marknadsplats online i art. 6.28 i cybersäkerhetsdirektivet.

I paragrafens 28 *punkt* definieras sökmotor: som en sökmotor enligt definitionen i art. 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (nedan kallad *plattformsförordningen*). Enligt plattformsförordningen avser en sökmotor en digital tjänst som gör det möjligt för användare att mata in sökfraser för att göra sökningar på i princip alla webbplatser eller alla webbplatser på ett visst språk på grundval av en fråga om vilket ämne som helst i form av ett nyckelord, en röstbegäran, en fras eller någon annan inmatning och som returnerar resultat i vilket format som helst som innehåller information om det begärda innehållet. Bestämmelsen genomför definitionen av sökmotor i art. 6.29 i cybersäkerhetsdirektivet.

I paragrafens 29 *punkt* definieras molntjänst: som en digital tjänst som 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. Bestämmelsen genomför definitionen av molntjänst i art. 6.30 i cybersäkerhetsdirektivet.

I paragrafens 30 *punkt* definieras datacentraltjänst som en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Bestämmelsen genomför definitionen av datacentraltjänst i art. 6.31 i cybersäkerhetsdirektivet.

I paragrafens 31 *punkt* definieras nätverk för leverans av innehåll som 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. Bestämmelsen genomför definitionen av nätverk för leverans av innehåll i art. 6.32 i cybersäkerhetsdirektivet.

I paragrafens 32 *punkt* definieras plattform för sociala nätverkstjänster som en plattform som 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. Bestämmelsen genomför definitionen av plattform för sociala nätverkstjänster i art. 6.33 i cybersäkerhetsdirektivet.

I paragrafens 33 *punkt* definieras *företrädare* som en i unionen etablerad fysisk eller juridisk person som 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 som inte är etablerad i unionen, till vilka tillsynsmyndigheten eller enheten för hantering av it-säkerhetsincidenter, vilka på Åland utgörs av landskapsregeringen, kan vända sig i stället för verksamhetsutövaren, i frågor som gäller de skyldigheter som verksamhetsutövaren har enligt denna lag. Bestämmelsen genomför definitionen av företrädare i art. 6.34 i cybersäkerhetsdirektivet.

I paragrafens 34 punkt definieras allmänt tillgänglig elektronisk kommunikationstjänst som en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och omfattar, med undantag av tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och kommunikationstjänster eller utövande av redaktionellt ansvar över sådant innehåll, nummeroberoende interpersonella kommunikationstjänster, vilka tillhandahålls till en grupp användare vilken inte har definierats på förhand. Med interpersonell kommunikationstjänst avses definitionen av interpersonell kommunikationstjänst i art. 2.5 i kodexdirektivet, vilket definieras som en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna; den inbegriper inte tjänster som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst. Med nummeroberoende interpersonell kommunikationstjänst avses definitionen av nummeroberoende interpersonell kommunikationstjänst i art. 2.7 i kodexdirektivet, vilket definieras som en interpersonell kommunikationstjänst som inte använder allmänt tilldelade nummerresurser, närmare bestämt ett eller flera nummer i nationella eller internationella nummerplaner, eller som inte möjliggör kommunikation med ett eller flera nummer i nationella eller internationella nummerplaner. Lagens definition av elektronisk kommunikationstjänst är snävare än den i cybersäkerhetsdirektivet, till följd av rikets lagstiftningsbehörighet över televäsendet, vilken inbegriper televerksamhet som internetanslutningstjänster, nummerberoende interpersonella kommunikationstjänster och tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster och för utsändningstjänster. Bestämmelsen genomför de delar av definitionen av elektroniska kommunikationstjänster, vilka faller under Åland lagstiftningsbehörighet, i art. 6.37 i cybersäkerhetsdirektivet, vari definitionen av elektronisk kommunikationstjänst kopplas till definitionen i art. 2.4 i kodexdirektivet.

I paragrafens 35 punkt definieras leverantör av utlokaliserade driftstjänster som en verksamhetsutövare som tillhandahåller tjänster som 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. Bestämmelsen genomför definitionen av leverantör av utlokaliserade driftstjänster i art. 6.39 i cybersäkerhetsdirektivet.

I paragrafens 36 punkt definieras leverantör av utlokaliserade säkerhetstjänster som en leverantör av utlokaliserade driftstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker. Bestämmelsen genomför definitionen av leverantör av utlokaliserade säkerhetstjänster i art. 6.40 i cybersäkerhetsdirektivet.

I paragrafens 37 punkt definieras forskningsorganisation som 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 som inte inbegriper utbildningsinstitutioner. Bestämmelsen genomför definitionen av forskning i art. 6.41 i cybersäkerhetsdirektivet.

I paragrafens 38 punkt definieras motståndskraft som en kritisk verksamhetsutövares förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident. Bestämmelsen genomför definitionen av motståndskraft i art. 2.2 i motståndskraftsdirektivet.

I paragrafens 39 *punkt* definieras kritisk infrastruktur som en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst. Bestämmelsen genomför definitionen av kritisk infrastruktur i art. 2.4 i motståndskraftsdirektivet.

I paragrafens 40 *punkt* definieras samhällsviktig tjänst som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. Bestämmelsen genomför definitionen av samhällsviktig tjänst i art. 2.5 i motståndskraftsdirektivet.

I paragrafens 41 *punkt* definieras verksamhetsutövare som en juridisk eller fysisk person, enskild eller offentlig, som bedriver verksamhet. Bestämmelsen genomför definitionen av entitet i art. 6.38 i cybersäkerhetsdirektivet.

I paragrafens 42 *punkt* definieras offentlig verksamhetsutövare som landskapsregeringen och under denna lydande myndigheter, med undantag för Ålands polismyndighet. Vidare undantas även andra offentliga verksamhetsutövare och delar av deras verksamheter eller tjänster enligt 4 § 1 och 2 mom., till följd av att de är verksamma inom områdena nationell säkerhet, allmän säkerhet, försvar och brottsbekämpning. Bestämmelsen genomför definitionen av offentlig förvaltningsentitet i art. 6.35 i cybersäkerhetsdirektivet jämte art. 2.10 i motståndskraftsdirektivet.

I paragrafens 43 *punkt* definieras nationell strategi för cybersäkerhet som Finlands nationella strategi för cybersäkerhet enligt 42 § cybersäkerhetslagen (FFS --:-- , nedan kallad *rikets cybersäkerhetslag*). Rikets bestämmelse om nationell strategi för cybersäkerhet utgör det nationella genomförandet av art. 7 i cybersäkerhetsdirektivet, enligt vilken varje medlemsstat ska 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. Definitionen motiveras av att en hänvisning till det nationella genomförandet i denna del behövs i lagtexten till följd av att föreskrifter om skyldigheter är kopplade till den nationella strategin, vilken alltså inte kan genomföras av landskapet själv till följd av rikets exklusiva behörighet enligt 59b § 2 mom. självstyrelselagen.

I paragrafens 44 *punkt* definieras nationell strategi för motståndskraft som Finlands nationella strategi för kritiska aktörers motståndskraft enligt 5 § lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft (FFS --:-- , nedan kallad *rikets motståndskraftslag*). Rikets bestämmelse om nationell strategi för kritiska aktörers motståndskraft utgör det nationella genomförandet av art. 4 i motståndskraftsdirektivet, enligt vilken varje medlemsstat efter samråd, om möjligt öppet för berörda parter, ska anta en strategi för att stärka kritiska entiteters motståndskraft. Strategin ska innehålla strategiska mål och policyåtgärder, som bygger på relevanta befintliga nationella och sektorsspecifika strategier, planer eller liknande dokument, för att uppnå och upprätthålla en hög grad av motståndskraft hos kritiska verksamhetsutövare. Definitionen motiveras av att en hänvisning till det nationella genomförandet i denna del behövs i lagtexten till följd av att föreskrifter om skyldigheter är kopplade till den nationella strategin, vilken alltså inte kan genomföras av landskapet själv till följd av rikets exklusiva behörighet enligt 59b § 2 mom. självstyrelselagen.

I paragrafens 45 *punkt* definieras nationell riskbedömning som Finlands nationella riskbedömning av kritisk infrastruktur och kritiska aktörers motståndskraft enligt 6 § rikets motståndskraftslag. Rikets bestämmelse om nationell riskbedömning utgör det nationella genomförandet av art. 5 i motståndskraftsdirektivet, enligt vilken behöriga myndigheter ska använda kommissionens förteckning över samhällsviktiga tjänster för att genomföra en riskbedömning. Medlemsstatens riskbedömning ska innehålla en

redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot, inklusive terroristbrott. Definitionen motiveras av att en hänvisning till det nationella genomförandet i denna del behövs i lagtexten till följd av att föreskrifter om skyldigheter är kopplade till den nationella riskbedömningen, vilken alltså inte kan genomföras av landskapet själv till följd av rikets exklusiva behörighet enligt 59b § 2 mom. självstyrelselagen.

I paragrafens *46 punkt* definieras NIS-samarbetsgruppen som samarbetsgruppen vilken har inrättats genom art. 14 i cybersäkerhetsdirektivet, enligt vilken NIS-samarbetsgruppen inrättas för att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna samt stärka förtroende och tillit.

I paragrafens *47 punkt* definieras CSIRT-nätverket som nätverket för enheter för hantering av cybersäkerhetsincidenter som har inrättats genom art. 15 i cybersäkerhetsdirektivet, enligt vilken CSIRT-nätverket inrättas för att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna.

I paragrafens *48 punkt* definieras EU-CyCLONe som det europeiska kontaktnätverket för cyberkriser vilket har inrättats genom art. 16 i cybersäkerhetsdirektivet, enligt vilken EU-CyCLONe inrättas för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

I paragrafens *49 punkt* definieras gruppen för kritiska entiteters motståndskraft som samarbetsgruppen vilken har inrättats genom art. 19 i motståndskraftdirektivet, enligt vilken gruppen för kritiska entiteters motståndskraft inrättas för att ge kommissionen stöd och underlätta samarbete mellan medlemsstaterna och informationsutbyte om frågor som rör motståndskraftsdirektivet.

I paragrafens *50 punkt* definieras sakkunnigbedömning som en sakkunnigbedömning enligt art. 19 i cybersäkerhetsdirektivet, enligt vilken sakkunnigbedömningar kan ordnas i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt stärka medlemsstaternas nödvändiga cybersäkerhetskapacitet och cybersäkerhetsriktlinjer för att genomföra cybersäkerhetsdirektivet.

I paragrafens *51 punkt* definieras rådgivande uppdrag som ett rådgivande uppdrag enligt art. 18 i motståndskraftsdirektivet, enligt vilken ett rådgivande uppdrag anordnas för att bedöma de åtgärder som den kritiska entiteten har infört för att uppfylla sina skyldigheter enligt motståndskraftsdirektivet.

2 kap. Lagens tillämpningsområde och begränsningar i det.

3 §. *Verksamhetsutövare.* I denna paragraf föreskrivs om lagens tillämpningsområde med avseende på enskilda och offentliga verksamhetsutövare.

I punktlistan i paragrafens *1 mom.* definieras de kriterier som var för sig kan göra lagens bestämmelser om cybersäkerhet tillämpliga vid en verksamhetsutövare vilka själva eller deras verksamhet, vilken inte är ringa eller sporadisk, omfattas av förteckningen i bilagorna I eller II till cybersäkerhetsdirektivet. Huruvida verksamheten är sporadisk och ringa ska bedömas i förhållande till verksamhetens varaktighet, huvudsakliga syfte och omfattning samt till antalet användare eller kunder vilka är beroende av verksamheten. Som sporadisk och ringa verksamhet bör exempelvis anses produktion av el vilken huvudsakligen sker för eget bruk med hjälp av en solpanel eller vindgenerator, där en kvantitativt liten överproduktion tidvis matas in i elnätet. Undantaget behövs för att lagens tillämpningsområde inte i strid med lagens

syfte ska utvidgas till att på grund av ringa eller tillfällig verksamhet, vilken avses i bilaga I eller II till cybersäkerhetsdirektivet, i sin helhet ska omfatta en juridisk eller fysisk person vars verksamhet annars uppfyller eller överstiger definitionen av en medelstor aktör, men som i övrigt inte skulle omfattas av lagens tillämpningsområde.

Av 1 mom. *1 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka 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. Bestämmelsen genomför art. 2.1 i cybersäkerhetsdirektivet.

Av 1 mom. *2 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst, enligt definitionen av allmänt tillgänglig elektronisk kommunikationstjänst enligt 2 § 34 punkten, eller en betrodd tjänst, enligt definitionen av betrodd tjänst enligt 2 § 23 punkten. Bestämmelsen genomför art. 2.2 led a.i och a.ii i cybersäkerhetsdirektivet.

Av 1 mom. *3 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka är den enda leverantören i Finland av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Bestämmelsen genomför art. 2.2 led b i cybersäkerhetsdirektivet.

Av 1 mom. *4 punkten* följer att lagen är tillämplig på verksamhetsutövare för vilka en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa. Bestämmelsen genomför art. 2.2 led c i cybersäkerhetsdirektivet.

Av 1 mom. *5 punkten* följer att lagen är tillämplig på verksamhetsutövare för vilka en störning av den tjänst som verksamhetsutövaren tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser. Bestämmelsen genomför art. 2.2 led d i cybersäkerhetsdirektivet.

Av 1 mom. *6 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka är kritiska 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 som är beroende av denna verksamhetsutövare. Bestämmelsen genomför art. 2.2 led e i cybersäkerhetsdirektivet.

Av 1 mom. *7 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka är offentliga verksamhetsutövare, enligt definitionen av offentlig verksamhetsutövare enligt 2 § 42 punkten. Bestämmelsen genomför art. 2.2 led f.i i cybersäkerhetsdirektivet.

Av 1 mom. *8 punkten* följer att lagen är tillämplig på verksamhetsutövare vilka har identifierats som en kritisk verksamhetsutövare av landskapsregeringen. I 10 § 1 mom. återfinns bestämmelser om landskapsregeringens identifiering av kritiska verksamhetsutövare. Bestämmelsen genomför art. 2.3 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att lagen även ska tillämpas på verksamhetsutövare om de eller deras verksamheter omfattas av förteckningen i bilagan till motståndskraftsdirektivet och har identifierats som kritiska verksamhetsutövare av landskapsregeringen. I 10 § 1 mom. återfinns bestämmelser om landskapsregeringens identifiering av kritiska verksamhetsutövare. I och med att de uppräknade sektorerna och verksamhetsutövarna i bilaga I och II till cybersäkerhetsdirektivet och bilagan till motståndskraftsdirektivet inte är helt överlappande måste denna grund för lagens tillämpning vid angivna verksamhetsutövare regleras särskilt. Bestämmelsen genomför art. 1.1 i motståndskraftsdirektivet.

4 §. *Avgränsning av tillämpningsområdet*. I denna paragraf föreskrivs om avgränsning av lagens tillämpningsområde. Genom paragrafens 1–3 mom.

utnyttjas det nationella handlingsutrymmet för tillämpningsrådet som art. 2.7–2.9 i cybersäkerhetsdirektivet och 1.7 i motståndskraftsdirektivet tillåter.

I paragrafens 1 *mom.* föreskrivs ett undantag från tillämpningen av vissa skyldigheter för verksamhetsutövare att vidta åtgärder och rapporterings-skyldigheter för cybersäkerhet och motståndskraft, inbegripet sammanhängande tillsyns- och efterlevnadskontroll, i fråga om verksamhet eller tjänster som tillhandahålls för tryggnad av försvaret, den nationella säkerheten, allmän ordning och säkerhet eller förebyggande av brott, brottsutredning och lagföring. Andra skyldigheter, som den för verksamhetsutövare att lämna uppgifter till landskapsregeringen för förteckning enligt 11 § gäller dock alltjämt. Bestämmelsen genomför art. 2.7 i cybersäkerhetsdirektivet och art. 1.6 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att lagen inte tillämpas på verksamhetsutövare vilka enbart bedriver sådan verksamhet eller tillhandahåller sådana tjänster som avses i 1 *mom.* Bestämmelsen genomför art. 2.8 i cybersäkerhetsdirektivet och art. 1.7 i motståndskraftsdirektivet.

I paragrafens 3 *mom.* föreskrivs en avvikelse från 1 och 2 *mom.*, vilken anger att lagen likväl ska tillämpas fullt ut om verksamhetsutövaren är en tillhandahållare av betrodda tjänster, enligt 2 § 24 punkten. Bestämmelsen genomför art. 2.9 i cybersäkerhetsdirektivet.

I paragrafens 4 *mom.* föreskrivs ett generellt undantag från skyldigheten att vidta åtgärder för att stärka motståndskraften enligt 4 kap., jämte landskapsregeringens europeiska samråd om dessa verksamhetsutövare enligt 33 § 2 *mom.*, samt därmed sammanhängande tillsyns- och efterlevnadskontroll enligt 8 kap., inte ska tillämpas vid kritiska verksamhetsutövare vilka är verksamma inom sektorn digital infrastruktur i bilagan till motståndskraftsdirektivet. Bestämmelsen genomför art. 8 i motståndskraftsdirektivet.

I paragrafens 5 *mom.* föreskrivs det om avgränsning av lagens tillämpning på så sätt att den inte förpliktar verksamhetsutövare eller myndigheter att lämna ut information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed. Momentet innehåller ingen begränsning för när det ska tillämpas, utan innefattar därmed såväl informationsutlämning mellan verksamhetsutövare och myndigheter samt internationellt informationsutbyte. Bestämmelsen genomför art. 2.11 i cybersäkerhetsdirektivet och art. 1.8 i motståndskraftsdirektivet.

5 §. *Förhållandet till annan lagstiftning.* I denna paragraf föreskrivs om lagens förhållande till rikets cybersäkerhetslag, rikets motståndskraftslag samt annan lagstiftning om riskhanterings- och rapporteringsskyldigheter samt sekretess- och dataskydd. Lagens tillämpningsområde är enligt förslaget omfattande och sektorsöverskridande, och skyldigheterna ska tillämpas horisontellt. Därför är det nödvändigt att förtydliga lagens förhållande till såväl rikets genomförande inom ramen för rikets behörighet samt annan lagstiftning om skyldighet att hantera cybersäkerhetsrisker och rapportera om dem. Syftet med paragrafen är att förtydliga lagens betydelse som allmän lag i förhållande till särskilda branschspecifika bestämmelser genom vilka en högre cybersäkerhetsnivå säkerställs. Om det finns särskilda branschspecifika bestämmelser i någon annan lag, ska de tillämpas i stället för motsvarande bestämmelser i den föreslagna lagen. I lagen föreskrivs det om de riskhanterings- och rapporteringsskyldigheter för varje bransch som miniminivån enligt cybersäkerhetsdirektivet förutsätter. Sektorsvis är det dock möjligt att det nationell eller unionsrättslig lagstiftning för en viss bransch eller typ av verksamhetsutövare uppställs mer detaljerade eller exakta skyldigheter som syftar till att säkerställa en högre nivå på cybersäkerheten än de allmänna skyldigheterna enligt cybersäkerhetsdirektivet. Sådana skyldigheter kan

exempelvis jämfört med denna lag innehålla mer detaljerade bestämmelser om de delområden som ska beaktas i riskhanteringen, förutsätta att en viss standard eller certifiering tillämpas, precisera eller justera en branschspecifik tröskel för incidenter som ska rapporteras till myndigheterna eller kräva en tätare eller snabbare rapportering till tillsynsmyndigheten. Sektorsspecifik reglering ska därmed tillämpas i stället för den föreslagna lagen till den del syftet med den sektorsspecifika regleringen är att säkerställa en högre cybersäkerhetsnivå.

I paragrafens *1 mom.* föreskrivs att lagens enbart ska tillämpas på verksamhetsutövare som omfattas av lagens tillämpningsområde till den del som dessa bedriva verksamhet eller tillhandahåller tjänster inom ramen för Ålands lagstiftningsbehörighet. I och med den delade behörigheten för genomförandet av cybersäkerhets- och motståndskraftsdirektiven på Åland är det viktigt att det förtydligas att lagen enbart ska tillämpas till den del som verksamhetsutövare verkar inom ramen för Ålands lagstiftningsbehörighet. I vissa fall kan detta i praktiken leda till att särskilt större eller verksamhetsutövare med en bred verksamhetsportfölj, vilka bedriver verksamheter på eller riktat till Åland inom såväl rikets som Ålands behörighetsområden, omfattas av såväl aktuell lag som av rikets genomförandelagstiftning till olika delar. I praktiken bör dock inte dylika fall leda till några större praktiska svårigheter vid verksamhetsutövarnas tillämpning av de olika materiella skyldigheterna, mot bakgrund av att såväl Åland som riket har gått in för direktivnära minimigenomföranden av aktuella direktiv. Det kan dock vid skarpa incidenter finnas särskilda behov av tydlighet för dessa verksamheter rörande vilka myndigheter de ska vända sig till för stöd och rapportering.

I paragrafens *2 mom.* föreskrivs det om lagens förhållande till de bestämmelser i nationell, åländsk eller unionsrättslig speciallagstiftning avseende krav på verksamhetsutövare om vidtagande av åtgärder för att stärka sin motståndskraft eller hantera cybersäkerhetsrisker eller rapportering av betydande cybersäkerhetsincidenter. Bestämmelsen uttrycker lagens förhållande både till nuvarande och kommande specialbestämmelser, att den som huvudregel ska avses vara en allmän lag i förhållande till branschspecifika eller aktörsspecifika specialbestämmelser någon annanstans i lag. I enlighet med art. 5 i cybersäkerhetsdirektivet och art. 3 i motståndskraftsdirektivet hindras inte en medlemsstat från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsskydds- eller motståndskraftnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten. Om det i en unionsrättslig, nationell eller åländsk lag eller i bestämmelser eller föreskrifter som utfärdats med stöd av en sådan finns branschspecifika krav, och kraven har minst samma verkan som motsvarande skyldigheter som fastställs i den föreslagna lagen, ska de tillämpas i stället för motsvarande bestämmelser i den föreslagna lagen. Avseende cybersäkerhet ska samma verkan som skyldigheterna i denna lag fastställas utifrån om åtgärderna är likvärda de som föreskrivs i 5 kap. och lagen i fråga föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentrapporter från enheter för hantering av cybersäkerhetsrisker och tillsynsmyndigheter samt den gemensamma kontaktpunkten enligt cybersäkerhetsdirektivet, det vill säga landskapsregeringen och Cybersäkerhetscentret vid Trafik- och kommunikationsverket, och om kraven på rapportering av betydande cybersäkerhetsincidenter har minst samma verkan som de som har fastställs i 5 kap. Kommissionen har enligt art. 4.3 i cybersäkerhetsdirektivet fått i uppgift att tillhandahålla riktlinjer som klargör tillämpningen av art. 4.1 och 4.2 och ska regelbundet se över dessa, med beaktande av eventuella synpunkter från NIS-samarbetsgruppen och Enisa. Bestämmelsen genomför art. 4 och 5 i cybersäkerhetsdirektivet och art. 1.3 och 3 i motståndskraftsdirektivet.

I paragrafens 3 *mom.* regleras att den information som är sekretessbelagd enligt unionsrättsliga eller andra bestämmelser enbart ska utbytas 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 verksamhetsutövers säkerhets- och affärsintressen. Bestämmelsen avgränsar därmed ytterligare informationsutlämningskyldigheterna enligt denna lag, i och med att den underkastas en bedömning från fall till fall utifrån behov, relevans, proportionerlighet för ändamålet med utbytet. Vidare ska skyddet av informationens konfidentialitet och berörda verksamhetsutövers säkerhets- och affärsintressen säkerställas. Bestämmelsen genomför art. 2.13 i cybersäkerhetsdirektivet och art. 1.4 i motståndskraftsdirektivet.

I paragrafens 4 *mom.* återfinns en informativ hänvisning till den allmänna dataskyddsförordningen och dataskyddslagarna, vari det föreskrivs närmare om datasäkerhet vid behandling av personuppgifter. Bestämmelsen genomför art. 2.12 och 2.14 i cybersäkerhetsdirektivet och art. 1.9 i motståndskraftsdirektivet.

6 §. *Jurisdiktion, territorialitet och gränsöverskridande verksamhetsutövare.* I denna paragraf föreskrivs det om den åländska jurisdiktionen, särskilt i förhållande till gränsöverskridande verksamhetsutövers samt deras verksamheters territorialitet.

I paragrafens 1 *mom.* föreskrivs huvudregeln att denna lag ska tillämpas på verksamhetsutövare som är etablerade och bedriver verksamhet eller tillhandahåller tjänster på Åland. Tillämpningsområdet för denna lag omfattar en verksamhetsutövare som är etablerad på Åland i sin helhet, det vill säga även de av verksamhetsutövers funktioner som finns till exempel i en annan medlemsstat eller i tredjeländer. Om en verksamhet som omfattas av tillämpningsområdet för denna lag bedrivs eller tjänster tillhandahålls på Åland av en verksamhetsutövare som är etablerad i en annan medlemsstat i Europeiska unionen, omfattas verksamhetsutövers därmed i regel och på motsvarande sätt av lagstiftningen och laglighetsövervakningen i etableringsstaten. Enligt art. 26.1 led c i cybersäkerhetsdirektivet omfattas en offentlig förvaltningsentitet alltid av jurisdiktionen i den medlemsstat som inrättade den. Bestämmelsen genomför art. 26.1 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs ett undantag från huvudregeln i 1 *mom.*, vilket anger att lagen alltså ska tillämpas vid gränsöverskridande digitala verksamhetsutövare som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst på Åland, oavsett etableringsstat. Bestämmelsen genomför art. 26.1 led a i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs ytterligare ett undantag från huvudregeln i 1 *mom.*, vilket anger att lagen ska tillämpas vid gränsöverskridande verksamhetsutövare som är leverantörer av molntjänster, datacentraltjänster, nätverk för leverans av innehåll, betrodda tjänster, allmänt tillgängliga elektroniska kommunikationstjänster, utlokaliserade drifttjänster, utlokaliserade säkerhetstjänster, internetbaserade marknadsplatser, sökmotorer eller plattformar för sociala nätverkstjänster, i den mån de har sitt huvudsakliga etableringsställe på Åland. För en gränsöverskridande verksamhetsutövare räcker det därmed inte att de är etablerade på Åland för att lagen ska tillämpas, utan att de dessutom har sitt huvudsakliga etableringsställe i Europeiska unionen på Åland, i enlighet med kriterierna i 4 *mom.* Bestämmelsen genomför art. 26.1 led b i cybersäkerhetsdirektivet.

I paragrafens 4 *mom.* föreskrivs att en gränsöverskridande verksamhetsutövare ska anses ha sitt huvudsakliga etableringsställe på Åland om det är inom landskapet beslutet om åtgärder för cybersäkerhet i huvudsak fattas. Om det inte kan fastställas att beslutet 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 som har flest anställda inom den Europeiska unionen. Bestämmelsen genomför art. 26.2 i cybersäkerhetsdirektivet.

I paragrafens 5 *mom.* regleras de fall där en gränsöverskridande verksamhetsutövare inte är etablerad i någon medlemsstat i Europeiska unionen. Om verksamhetsutövaren har sitt huvudsakliga verksamhetsställe utanför Europeiska unionen men tillhandahåller tjänster inom Europeiska unionen, förutsätts verksamhetsutövaren i enlighet med art. 26.3 i cybersäkerhetsdirektivet utse en företrädare i Europeiska unionen. Den namngivna företrädaren ska agera på verksamhetsutövarens vägnar, och det ska vara möjligt för de landskapsregeringen att vända sig till företrädaren. Företrädaren ska utses uttryckligen genom en skriftlig fullmakt från verksamhetsutövaren att agera på dess vägnar med avseende på dess skyldigheter enligt denna lag, inklusive incidentrapportering. Att utse en företrädare ska dock inte påverka medlemsstaternas möjligheter att vidta rättsliga åtgärder mot verksamhetsutövaren själv. Enligt bestämmelsen ska lagen tillämpas på verksamhetsutövaren om dess utsedda företrädare i Europeiska unionen är etablerad på Åland. För gränsöverskridande verksamhetsutövare som tillhandahåller tjänster på Åland, men inte har utsett en företrädare i Europeiska unionen, tillämpas alltjämt bestämmelserna i denna lag. En verksamhetsutövare som är etablerad utanför Europeiska unionen anses tillhandahålla tjänster inom Europeiska unionen om den avser att tillhandahålla tjänster till personer i en eller flera medlemsstater. Till exempel användning av ett språk eller en myntenhet som allmänt används i en eller flera medlemsstater och möjligheten att beställa tjänster på detta språk eller omnämnande av kunder eller användare i unionen kan visa att verksamhetsutövaren har för avsikt att tillhandahålla tjänster till personer i en medlemsstat i unionen. Det är dock i allmänhet inte tillräckligt att enbart ha tillgång till webbplatser, e-postadresser eller andra kontaktuppgifter i unionen för att visa att en verksamhetsutövare avser att tillhandahålla sina tjänster i unionen. Bestämmelsen genomför art. 26.3 i cybersäkerhetsdirektivet.

I paragrafens 6 *mom.* föreskrivs det om landskapsregeringens möjlighet att rikta tillsyns- och efterlevnadskontrollåtgärder mot en aktör som är etablerad i en annan medlemsstat i Europeiska unionen, men som tillhandahåller tjänster på Åland eller som har ett nätverks- eller informationssystem på Åland. Landskapsregeringen kan 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. En ytterligare förutsättning är att verksamhetsutövaren tillhandahåller tjänster på Åland eller har ett nätverks- eller informationssystem på åländskt territorium och att landskapsregeringen har rätt att vidta den begärda åtgärden med stöd av denna lag. Bestämmelsen genomför art. 26.5 i cybersäkerhetsdirektivet.

3 kap. Klassificering, identifiering och informering av verksamhetsutövare.

7 §. *Kritiska verksamhetsutövare.* I denna paragraf föreskrivs om kriterierna för att en verksamhetsutövare av landskapsregeringen ska kunna identifieras som en kritisk verksamhetsutövare eller klassificeras som en kritisk verksamhetsutövare av särskild europeisk betydelse.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen, med iakttagande av rikets nationella riskbedömning, enligt definitionen i 2 § 45 punkten och

nationella strategi för motståndskraft, enligt definitionen i 2 § 44 punkten, kan identifiera en verksamhetsutövare som omfattas av förteckningen i bilagan till motståndskraftsdirektivet, utifrån kriterierna i punkterna 1–3. Samtliga kriterier ska tillämpas vid landskapsregeringens bedömning. Bestämmelsen genomför art. 2.1 och 6.2 i motståndskraftsdirektivet.

Enligt 1 mom. *1–3 punkterna* kan en verksamhetsutövare identifieras som kritisk om den tillhandahåller en eller flera samhällsviktiga tjänster, verksamhetsutövaren bedriver verksamhet och dess kritiska infrastruktur är belägen på Åland, och 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. Kommissionen har med stöd av artikel 5.1 i motståndskraftsdirektivet upprättat en icke uttömmande förteckning över samhällsviktiga tjänster i Kommissionens delegerade förordning (EU) 2023/2450 om komplettering av Europaparlamentets och rådets direktiv (EU) 2022/2557 genom upprättande av en förteckning över samhällsviktiga tjänster.

I paragrafens *2 mom.* föreskrivs de omständigheter utifrån vilka landskapsregeringens bedömning av huruvida en incident skulle få betydande störande effekter enligt 1 mom. 3 punkten. Samtliga kriterier ska tillämpas vid landskapsregeringens bedömning.

Enligt 2 mom. *1–6 punkterna* ska landskapsregeringen beakta antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamhetsutövaren tillhandahåller, den grad till vilken andra verksamhetsutövare är beroende av den samhällsviktiga tjänsten i fråga, vilken effekt incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa, uttryckt i grad och varaktighet, verksamhetsutövarens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna, det geografiska område som skulle kunna påverkas av en incident, inbegripet eventuella gränsöverskridande konsekvenser, med beaktande av den sårbarhet som är förknippad med graden av isolering för vissa typer av geografiska områden, såsom öregioner, avlägsna områden eller bergsområden, och verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att tillhandahålla den samhällsviktiga tjänsten. Bestämmelsen genomför art. 7.1 i motståndskraftsdirektivet.

I paragrafens *3 mom.* föreskrivs att en verksamhetsutövare ska klassificeras som en kritisk verksamhetsutövare av särskild europeisk betydelse om den av landskapsregeringen har identifierats som en kritisk verksamhetsutövare, och 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. Bestämmelsen genomför art. 17.1 och 17.3 i motståndskraftsdirektivet.

8 §. Väsentliga verksamhetsutövare. I denna paragraf föreskrivs om kriterierna för att en verksamhetsutövare ska klassificeras som en väsentlig verksamhetsutövare, varav endast ett behöver uppfyllas för att klassificeringen ska inträda.

Paragrafens *1 punkt* omfattar verksamhetsutövare vilka 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. Bestämmelsen genomför art. 3.1 led a i cybersäkerhetsdirektivet.

Paragrafens 2 punkt omfattar verksamhetsutövare vilka är en tillhandahållare av allmänt tillgängliga elektroniska kommunikations-tjänster och definieras som ett medelstort företag enligt artikel 2 i bilagan till Kommissionens rekommendation om definitionen av mikroföretag samt små och medelstora företag. Bestämmelsen genomför art. 3.1 led c i cybersäkerhetsdirektivet.

Paragrafens 3 punkt omfattar verksamhetsutövare vilka är en kvalificerad tillhandahållare av betrodda tjänster. Bestämmelsen genomför art. 3.1 led b i cybersäkerhetsdirektivet.

Paragrafens 4 punkt omfattar verksamhetsutövare vilka är en offentlig verksamhetsutövare enligt definitionen i 2 § 42 punkten. Bestämmelsen genomför art. 3.1 led d i cybersäkerhetsdirektivet.

Paragrafens 5 punkt omfattar verksamhetsutövare vilka av landskapsregeringen har identifierats som en kritisk verksamhetsutövare enligt 7 och 10 §§. Bestämmelsen genomför art. 3.1 led f i cybersäkerhetsdirektivet.

Paragrafens 6 punkt omfattar verksamhetsutövare vilka av landskapsregeringen enligt 10 §, utifrån kriterierna i 3 § 3–6 punkterna har identifierats som en väsentlig verksamhetsutövare. Bestämmelsen föreskriver vidare genom hänvisning kriterierna för landskapsregeringens identifiering av en verksamhetsutövare som väsentlig. Bestämmelsen genomför art. 3.1 led e i cybersäkerhetsdirektivet.

9 §. *Viktiga verksamhetsutövare.* I denna paragraf föreskrivs att verksamhetsutövare vilka omfattas av förteckningen 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 enligt 10 §, utifrån kriterierna i 3 § 3–6 punkterna, har identifierats som viktiga verksamhetsutövare. Bestämmelsen träffar därmed verksamhetsutövare vilka omfattas av lagens tillämpningsområde enligt 3 § 1 mom. men inte klassificerats som väsentliga verksamhetsutövare eller av landskapsregeringen har identifierats som sådana. Framst handlar det om verksamhetsutövare vilka uppfyller storlekskraven för medelstora företag och omfattas av endera bilaga I eller II till cybersäkerhetsdirektivet, samt i andra hand de vilka av landskapsregering identifieras som viktiga verksamhetsutövare. Bestämmelsen föreskriver vidare genom hänvisning kriterierna för landskapsregeringens identifiering av en verksamhetsutövare som viktig. Bestämmelsen genomför art. 3.2 i cybersäkerhetsdirektivet.

10 §. *Landskapsregeringens identifiering av verksamhetsutövare och underrättelse om detta.* I denna paragraf föreskrivs om landskapsregeringens skyldighet att innan de tidsfrister som föreskrivs i direktiven identifiera verksamhetsutövare som omfattas av förteckningarna i bilagorna I och II till cybersäkerhetsdirektivet och bilagan till motståndskraftsdirektivet som kritiska, väsentliga och viktiga verksamhetsutövare, samt underrättelser om landskapsregeringens identifiering till dessa.

I paragrafens 1 mom. föreskrivs att landskapsregeringen senast den 17 juli 2026, samt därefter när så är nödvändigt, utifrån kriterierna i 7 § ska identifiera verksamhetsutövare vilka omfattas av förteckningen i bilagan till motståndskraftsdirektivet som kritiska verksamhetsutövare. Bestämmelsen genomför art. 6.1 och 6.3 i motståndskraftsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen senast den 17 april 2025, samt därefter när så är nödvändigt, identifiera andra än redan klassificerade verksamhetsutövare vilka omfattas av förteckningen i bilagorna I och II till cybersäkerhetsdirektivet som en väsentlig eller viktig verksamhetsutövare. Bestämmelsen genomför art. 3.1 led e och 3.3 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att landskapsregeringen är skyldig att underrätta de verksamhetsutövare som 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 som 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 identifiering, med undantag för identifierade kritiska verksamhetsutövare av särskild europeisk betydelse, vilka ska underrättas utan dröjsmål. Bestämmelsen genomför art. 6.3, 6.4, 17.3 och 17.4 i motståndskraftsdirektivet. Motsvarande bestämmelser om tidsfrist för underrättelser till identifierade verksamhetsutövare saknas i cybersäkerhetsdirektivet. Behov av underrättelse om identifiering till berörda verksamhetsutövare föreligger dock även i förhållande till väsentliga och viktiga verksamhetsutövare, utifrån deras behov av att få klarhet om vilka skyldigheter som åligger dem enligt denna lag, varför regleringen görs enhetlig.

11 §. *Uppgifter om verksamhetsutövare för förteckning.* I denna paragraf föreskrivs om klassificerade eller identifierade verksamhetsutövares skyldigheter att lämna uppgifter till landskapsregeringen om sig själva och deras berörda verksamheter.

I paragrafens 1 *mom.* föreskrivs att en verksamhetsutövare som har klassificerats eller identifierats som en väsentlig eller viktig verksamhetsutövare åtminstone ska lämna relevanta uppgifter till landskapsregeringen, inbegripet namn, adress och aktuella kontaktuppgifter, inklusive e-postadresser, IP-adresser och telefonnummer, den eller de sektorer och undersektorer enligt förteckningen i bilagorna I eller II i cybersäkerhetsdirektivet som verksamhetsutövaren tillhör, och, i tillämpliga fall, en förteckning över de medlemsstater i Europeiska unionen där de tillhandahåller tjänster som omfattas av cybersäkerhetsdirektivet. Bestämmelsen genomför art. 3.4 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att verksamhetsutövare enligt 1 *mom.* vilka är leverantörer av molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, internetbaserade marknadsplatser, sökmotorer och plattformar för sociala nätverkstjänster även, och senast den 17 januari 2025, ska lämna uppgift till landskapsregeringen om den typ av verksamhetsutövare enligt förteckningen i bilagorna I eller II i cybersäkerhetsdirektivet vilken verksamhetsutövaren utgör, 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 verksamhetsutövarens IP-adressintervall. Bestämmelsen genomför art. 27.2 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att berörda verksamhetsutövare utan dröjsmål ska underrätta landskapsregeringen om ändringar av de uppgifter som avses i 1 och 2 *mom.* i paragrafen. Landskapsregeringen ska underrättas om ändringar av de uppgifter som avses i 1 *mom.* inom två veckor och av de uppgifter som avses i 2 *mom.* inom tre månader från datumet för ändringen. Bestämmelsen genomför art. 3.4 och 27.3 i cybersäkerhetsdirektivet.

I paragrafens 4 *mom.* föreskrivs att 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 som den tillhandahåller till eller i dessa medlemsstater och till eller i vilka medlemsstater den tillhandahåller sådana samhällsviktiga tjänster. Bestämmelsen genomför art. 17.2 1 *mom.* i motståndskraftsdirektivet.

12 §. *Landskapsregeringens informationsutlämning för förteckning och till kommissionen.* I denna paragraf föreskrivs om landskapsregeringens skyldigheter att lämna uppgifter om klassificerade eller identifierade verksamhetsutövare till de gemensamma kontaktpunkterna vid Försörjningsberedskapscentralen och Cybersäkerhetscentret vid Transport- och kommunikationsverket för upprättande av den nationella förteckningen över verksamhetsutövare och för fullgörandet av deras övriga uppgifter enligt cybersäkerhets- och motståndskraftsdirektiven, samt landskapsregeringens utlämnande av motsvarande information till kommissionen.

I paragrafens *1 mom.* föreskrivs att landskapsregeringen senast den 17 juli 2026 till Finlands gemensamma kontaktpunkt Försörjningsberedskapscentralen ska överlämna samtliga de uppgifter vilka den behöver för att upprätta den nationella förteckningen över kritiska verksamhetsutövare och fullgöra sina övriga uppgifter som gemensam kontaktpunkt enligt motståndskraftsdirektivet. Bestämmelsen motiveras av rikets exklusiva behörighet att upprätta förteckningen enligt 59b § 2 mom. självstyrelselagen. Bestämmelsen genomför art. 6.3 i motståndskraftsdirektivet.

I paragrafens *2 mom.* föreskrivs att landskapsregeringen senast den 17 april 2025 till Finlands gemensamma kontaktpunkt vid Cybersäkerhetscentret vid Transport- och kommunikationsverket ska överlämna samtliga de uppgifter vilka den behöver för att upprätta en förteckning över väsentliga och viktiga verksamhetsutövare och fullgöra sina övriga uppgifter som gemensam kontaktpunkt enligt cybersäkerhetsdirektivet. Bestämmelsen motiveras av rikets exklusiva behörighet att upprätta förteckningen enligt 59b § 2 mom. självstyrelselagen. Bestämmelsen genomför art. 3.3 i cybersäkerhetsdirektivet.

I paragrafens *3 mom.* föreskrivs att landskapsregeringen senast den 17 april 2025 och därefter vartannat år genom ansvarig riksmyndighet ska underrätta kommissionen och NIS-samarbetsgruppen om antalet väsentliga och viktiga entiteter som har förtecknats enligt 2 mom. för varje sektor och undersektor som avses i förteckningen i bilagorna I eller II till cybersäkerhetsdirektivet, och lämna relevant information till kommissionen om antalet väsentliga och viktiga verksamhetsutövare som 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 som de tillhandahåller och de grunder enligt artikel 2.2 b–e i cybersäkerhetsdirektivet i enlighet med vilka de identifierades. Att kommunikationen ska ske genom ansvarig riksmyndighet motiveras av rikets exklusiva behörighet över förhållandet till utländska makter enligt 27 § 4 punkten självstyrelselagen. Bestämmelsen genomför art. 3.5 i cybersäkerhetsdirektivet.

I paragrafens *4 mom.* föreskrivs att landskapsregeringen fram till den 17 april 2025 och på begäran av kommissionen genom ansvarig riksmyndighet får meddela namnen på de väsentliga och viktiga verksamhetsutövare som avses i 3 mom. 2 punkten. Bestämmelsen genomför art. 3.6 i cybersäkerhetsdirektivet.

I paragrafens *5 mom.* föreskrivs att landskapsregeringen utan onödigt dröjsmål ska underrätta kommissionen ansvarig riksmyndighet om identiteten på kritiska verksamhetsutövare som kan utgöra kritiska verksamhetsutövare av europeisk betydelse samt om den information som verksamhetsutövaren har tillhandahållit om dess tillhandahållande av samhällsviktiga tjänster som är av betydelse för denna bedömning. Vid efterföljande samråd med kommissionen ska landskapsregeringen informera kommissionen om den bedömer att de tjänster som en kritisk verksamhetsutövare tillhandahåller på Åland är samhällsviktiga tjänster. Bestämmelsen genomför art. 17.2 i motståndskraftsdirektivet.

4 kap. Kritiska verksamhetsutövares skyldigheter

13 §. *Riskbedömning.* I denna paragraf föreskrivs om en kritisk verksamhetsutövares skyldighet att göra en riskbedömning för att bedöma alla relevanta risker som kan störa tillhandahållandet av dess samhällsviktiga tjänster.

I paragrafens 1 mom. ska en kritisk verksamhetsutövare 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 som kan störa tillhandahållandet av dess samhällsviktiga tjänster. Dessa andra informationskällor kan vara information och bedömningar av hot eller andra aspekter av motståndskraft från landskapsregeringen eller en annan myndighet samt information om och erfarenheter av inträffade incidenter. Utgångspunkten är således att en kritisk verksamhetsutövare ska göra en samlad bedömning av de relevanta risker som den är utsatt för, för vilken den ska göra riskbedömningar när det är nödvändigt med hänsyn till dess specifika omständigheter och riskernas utveckling, och under alla omständigheter vart fjärde år. Bestämmelsen genomför art. 12.1 i motståndskraftsdirektivet.

I paragrafens 2 mom. föreskrivs att en riskbedömning enligt 1 mom. ska innehålla en redogörelse för alla relevanta risker för naturolyckor och risker orsakade av människan som skulle kunna leda till en incident, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inbegripet terroristbrott. Bestämmelsen genomför art. 12.2 mom. 1 men. 1 i motståndskraftsdirektivet.

I paragrafens 3 mom. föreskrivs att 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 som tillhandahålls av den kritiska verksamhetsutövaren och den grad till vilken den är beroende av samhällsviktiga tjänster som tillhandahålls av andra verksamhetsutövare i sådana andra sektorer, inbegripet i angränsande medlemsstater i Europeiska unionen och, i förekommande fall, tredjeländer. Bestämmelsen genomför art. 12.2 mom. 1 men. 2 i motståndskraftsdirektivet.

I paragrafens 4 mom. föreskrivs att en kritisk verksamhetsutövare får, om en annan riskbedömning eller ett annat dokument utarbetats för motsvarande ändamål, använda den bedömningen eller det dokumentet i stället. Bestämmelsen genomför art. 12.2 mom. 2 men. 1 i motståndskraftsdirektivet.

I paragrafens 5 mom. föreskrivs att landskapsregeringen inom ramen för utövandet av sin tillsynsfunktion kan slå fast att en annan riskbedömning utarbetad av en kritisk verksamhetsutövare helt eller delvis uppfyller skyldigheten enligt denna paragraf. Bestämmelsen genomför art. 12.2 mom. 2 men. 2 i motståndskraftsdirektivet.

14 §. *Åtgärder och plan för motståndskraft.* I denna paragraf föreskrivs skyldigheter för en kritisk verksamhetsutövare att vidta åtgärder för säkerställande av sin motståndskraft samt att utarbeta en plan för motståndskraft.

I paragrafens 1 mom. föreskrivs att 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, vilka är nödvändiga för att uppnå de mål som anges i punktlistan. Bestämmelsen genomför art. 13.1 i motståndskraftsdirektivet.

Enligt 1 mom. 1 punkten ska den kritiska verksamhetsutövaren vidta åtgärder vilka är nödvändiga för att förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning.

Enligt 1 mom. 2 *punkten* ska en kritisk verksamhetsutövare vidta åtgärder vilka är nödvändiga för att säkerställa ett tillfredsställande fysiskt skydd av dess lokaler och kritiska infrastruktur, med vederbörlig hänsyn till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller.

Enligt 1 mom. 3 *punkten* ska en kritisk verksamhetsutövare vidta åtgärder vilka är nödvändiga för att reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner,

Enligt 1 mom. 4 *punkten* ska en kritisk verksamhetsutövare vidta åtgärder vilka är nödvändiga för att återhämta sig från incidenter, med vederbörlig hänsyn till åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten.

Enligt 1 mom. 5 *punkten* ska en kritisk verksamhetsutövare vidta åtgärder vilka är nödvändiga för att säkerställa en ändamålsenlig hantering av personalsäkerhet, med vederbörlig hänsyn till åtgärder såsom fastställande av kategorier av personal som utför kritiska funktioner, med beaktande av externa tjänsteleverantörers personal, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer.

Enligt 1 mom. 6 *punkten* ska en kritisk verksamhetsutövare vidta åtgärder vilka är nödvändiga för att öka medvetenheten om åtgärderna hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

I paragrafens 2 *mom.* föreskrivs att en kritisk verksamhetsutövare i samma syfte ska utarbeta en plan för motståndskraft, innehållande en beskrivning av de åtgärder som har vidtagits enligt 1 mom. Bestämmelsen genomför art. 13.2 men. 1 i motståndskraftsdirektivet.

I paragrafens 3 *mom.* föreskrivs att 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

I paragrafens 4 *mom.* föreskrivs att landskapsregeringen inom ramen för utövandet av sin tillsynsfunktion kan slå fast att en annan plan eller ett annat dokument utarbetat av en kritisk verksamhetsutövare helt eller delvis uppfyller skyldigheten enligt denna paragraf. Bestämmelsen genomför art. 13.2 men. 3 i motståndskraftsdirektivet.

I paragrafens 5 *mom.* föreskrivs att en kritisk verksamhetsutövare ska utse en kontaktpunkt, genom vilken sambandet med landskapsregeringen ordnas. Bestämmelsen genomför art. 13.3 i motståndskraftsdirektivet.

I paragrafens 6 *mom.* återfinns ett förordningsbemyndigande för landskapsregeringen om utfärdande av närmare bestämmelser om åtgärder och plan för motståndskraft enligt 1 och 2 mom.

15 §. *Säkerhetsutredning.* Denna paragraf innehåller en information hänvisning om att en kritisk verksamhetsutövare har möjlighet att ansöka om säkerhetsutredning av en person enligt säkerhetsutredningslagen (FFS 726/2014) hos däri angiven riksmyndighet, vilken är Skyddspolisen. Ansökan om säkerhetsutredning av en person görs av sökanden, det vill säga verksamhetsutövaren, i enlighet med förutsättningarna i 18 § och 19 § 4 punkten och ska vidare uppfylla formkraven enligt 17 § säkerhetsutredningslagen. Bestämmelsen genomför tillsammans med rikets bestämmelser art. 14.1–14.3 i motståndskraftsdirektivet.

16 §. *Incidentrapportering.* I denna paragraf föreskrivs om kritiska verksamhetsutövares incidentrapporteringsskyldighet.

I paragrafens 1 mom. föreskrivs att en kritisk verksamhetsutövare utan onödigt dröjsmål ska rapportera till landskapsregeringen om incidenter som 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 omständigheter som antal och andel användare som berörs av störningen, störningens varaktighet, och det geografiska område som påverkas av störningen, med beaktande av huruvida området är geografiskt isolerat, beaktas. Bestämmelsen genomför art. 15.1 mom. 1 i motståndskraftsdirektivet.

I paragrafens 2 mom. föreskrivs att en incidentrapport enligt 1 mom. ska omfatta all tillgänglig information som är nödvändig för att landskapsregeringen ska kunna förstå incidentens art, orsak och möjliga konsekvenser, inbegripet eventuell information som krävs för att kunna fastställa incidentens eventuella gränsöverskridande verkningar. En incidentrapport medför inte ett ökat ansvar för en kritisk verksamhetsutövare. Bestämmelsen genomför art. 15.2 i motståndskraftsdirektivet.

I paragrafens 3 mom. återfinns ett förordningsbemyndigande för landskapsregeringen om utfärdande av närmare bestämmelser om formen för och innehållet i incidentrapportering enligt 1 och 2 mom.

17 §. *Standarder.* I denna paragraf föreskrivs att en kritisk verksamhetsutövare ska sträva efter att i förekommande fall använda tillämpliga europeiska och internationellt erkända standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft. Bestämmelsen genomför art. 16 i motståndskraftsdirektivet.

18 §. *Rådgivande uppdrag.* I denna paragraf föreskrivs om kritiska verksamhetsutövares skyldigheter i förhållande till rådgivande uppdrag.

I paragrafens 1 mom. föreskrivs att en berörd kritisk verksamhetsutövare av särskild europeisk betydelse till ett rådgivande uppdrag ska ge åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster som är nödvändiga för utförandet av ett rådgivande uppdrag. Bestämmelsen genomför art. 18.7 i motståndskraftsdirektivet.

I paragrafens 2 mom. föreskrivs att 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 som den har vidtagit i enlighet med yttrandet. Bestämmelsen genomför art. 18.4 mom. 4 i motståndskraftsdirektivet.

5 kap. Väsentliga och viktiga verksamhetsutövares skyldigheter

19 §. *Ledningens styrning och ansvar.* I denna paragraf föreskrivs om väsentliga och viktiga verksamhetsutövares ledningars styrning och ansvar.

I paragrafens 1 mom. föreskrivs att väsentlig eller viktig verksamhetsutövares ledning svarar för verksamhetsutövarens vidtagande av åtgärder för cybersäkerhet enligt 20 §, att lämpliga resurser avsätts för dem och övervakar deras genomförande och genomslag. Bestämmelsen genomför delar av art. 20.1, 32.6 och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. definieras ledning enligt 1 mom. som verksamhetsutövarens styrelse, förvaltningsråd och verkställande direktör samt någon

annan i därmed jämförbar ställning som i praktiken leder dess verksamhet. En sådan ställning kan till exempel innehas av en bolagsman i ett öppet bolag, en ansvarig bolagsman i ett kommanditbolag, en personmedlem i en europeisk ekonomisk intressegruppering eller en enskild näringsidkare. Bestämmelsen genomför delar av art. 20.1, 32.6 och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att en väsentlig eller viktig verksamhetsutövares ledning och dess befattningshavare kan ställas till svars för verksamhetsutövares överträdelse av dess skyldigheter enligt lagen. Ledningens försummelse av ansvaret kan leda till att aktören påförs en administrativ påföljd enligt denna lag. Hos en väsentlig aktör kan en allvarlig och upprepad försummelse av ledningens ansvar också leda till ett sådant beslut av tillsynsmyndigheten som avses i 8 kap. och som förbjuder en person att för viss tid sköta uppgifter som avses i denna paragraf. För tydlighetens skull konstateras det att det föreskrivs särskilt om skadeståndsansvar för bolagets ledning och dess befattningshavare. Bestämmelsen genomför delar av art. 20.1, 32.6 och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 4 *mom.* föreskrivs att en befattningshavare i en ledning är skyldig att genomgå relevant utbildning, och ska uppmuntra verksamhetsutövaren att regelbundet erbjuda liknande utbildning till sina anställda, vilken ska ge dem kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av verksamhetsutövaren. Bestämmelsen genomför art. 20.2 i cybersäkerhetsdirektivet.

20 §. *Åtgärder för cybersäkerhet.* I denna paragraf föreskrivs om väsentliga och viktiga verksamhetsutövares skyldigheter att vidta riskhanteringsåtgärder för cybersäkerhet.

I paragrafens 1 *mom.* föreskrivs att en väsentlig eller viktiga verksamhetsutövare ska vidta lämpliga och proportionerliga tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som 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. Bestämmelsen genomför art. 21.1 *mom.* 1 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att åtgärder enligt 1 *mom.* ska säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken, med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna. 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, inbegripet deras samhällsliga och ekonomiska konsekvenser. Bestämmelsen genomför art. 21.1 *mom.* 2 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att åtgärderna enligt 1 *mom.* ska baseras på en allriskansats som syftar till att skydda en verksamhetsutövares nätverks- och informationssystem samt dessa systems fysiska miljö från cybersäkerhetsincidenter, och ska åtminstone inbegripa de åtgärder som framgår av punktlistan. Bestämmelsen genomför art. 21.2 i cybersäkerhetsdirektivet. Kommissionen ska enligt art. 21.5 i cybersäkerhetsdirektivet senast den 17 oktober 2024 anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de åtgärder som avses i punktlistan i art. 21.2 för verksamhetsutövare inom sektorerna digital infrastruktur, förvaltning av IKT-tjänster (mellan företag) och digitala leverantörer, samt har möjlighet att utfärda andra sektorskrav även för andra typer av

verksamhetsutövare, i enlighet med granskningsförfarandet enligt art. 39.2 i cybersäkerhetsdirektivet.

Enligt 3 mom. 1 punkten ska verksamhetsutövare anta strategier för riskanalys och informationssystemens säkerhet.

Enligt 3 mom. 2 punkten ska verksamhetsutövare bedriva incidenthantering.

Enligt 3 mom. 3 punkten ska verksamhetsutövare tillförsäkra driftskontinuitet, exempelvis genom hantering av säkerhetskopiering och katastrofhantering, och krishantering.

Enligt 3 mom. 4 punkten ska verksamhetsutövare tillförsäkra säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje verksamhetsutövare och dess direkta leverantörer eller tjänsteleverantörer,

Enligt 3 mom. 5 punkten ska verksamhetsutövare tillförsäkra säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripande hantering av sårbarheter och sårbarhetsinformation,

Enligt 3 mom. 6 punkten ska verksamhetsutövare anta strategier och förfaranden för att bedöma effektiviteten i åtgärderna för cybersäkerhet,

Enligt 3 mom. 7 punkten ska verksamhetsutövare följa grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

Enligt 3 mom. 8 punkten ska verksamhetsutövare anta strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

Enligt 3 mom. 9 punkten ska verksamhetsutövare säkerställa personalsäkerhet, anta strategier för åtkomstkontroll och tillgångsförvaltning, och

Enligt 3 mom. 10 punkten ska verksamhetsutövare använda, när så är lämpligt, lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

I paragrafens 4 mom. föreskrivs att övervägande av lämpliga åtgärder enligt 3 mom. 4 punkten ska ske med beaktande av de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör, den övergripande kvaliteten på leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling och resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs av NIS-samarbetsgruppen i samarbete med kommissionen och Enisa. Bestämmelsen genomför art. 21.3 i cybersäkerhetsdirektivet.

I paragrafens 5 mom. föreskrivs att en väsentlig eller viktig verksamhetsutövare som finner att den inte följer de åtgärder som föreskrivs i 3 mom. ska utan onödigt dröjsmål vidta alla nödvändiga, lämpliga och proportionella korrigerande åtgärder. Bestämmelsen genomför art. 21.4 i cybersäkerhetsdirektivet.

I paragrafens 6 mom. återfinns ett förordningsbemyndigande för landskapsregeringen om utfärdande av närmare bestämmelser om åtgärder för cybersäkerhet enligt 1–4 mom.

21 §. *Cybersäkerhetsincidentrapportering.* I denna paragraf föreskrivs om väsentliga och viktiga verksamhetsutövares cybersäkerhetsincidentrapportering.

I paragrafens 1 mom. föreskrivs att en väsentlig eller viktig verksamhetsutövare utan onödigt dröjsmål ska 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. En berörd verksamhetsutövare ska bland annat rapportera information vilken gör det möjligt för landskapsregeringen att fastställa

cybersäkerhetsincidentens eventuella gränsöverskridande verkningar. Rapporteringen ska inte medföra ökat ansvar för den underrättande verksamhetsutövaren. Bestämmelsen genomför art. 23.1 mom. 1 i cybersäkerhetsdirektivet. Kommissionen får enligt art. 23.11 mom. 1 i cybersäkerhetsdirektivet anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med art. 23.1 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att verksamhetsutövaren även, i tillämpliga fall, utan onödigt dröjsmål ska underrätta de användare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa användare kan vidta som svar på hotet. När så är lämpligt ska verksamhetsutövaren även informera användare om det betydande cyberhotet. Bestämmelsen genomför art. 23.2 i cybersäkerhetsdirektivet. Kommissionen får enligt art. 23.11 mom. 1 i cybersäkerhetsdirektivet anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med art. 23.2 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att en cybersäkerhetsincident ska anses vara betydande om den antingen har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för verksamhetsutövaren, eller den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. Bestämmelsen genomför art. 23.3 i cybersäkerhetsdirektivet. Kommissionen ska enligt art. 23.11 mom. 1 i cybersäkerhetsdirektivet senast den 17 oktober 2024 anta genomförandeakter som närmare anger i vilka fall cybersäkerhetsincidenter som berör verksamhetsutövarna inom sektorerna digital infrastruktur, förvaltning av IKT-tjänster (mellan företag) och digitala leverantörer ska anses vara betydande. Kommissionen får även anta sådana genomförandeakter med avseende på andra väsentliga och viktiga verksamhetsutövare.

I paragrafens 4 mom. föreskrivs att verksamhetsutövaren vid rapportering enligt 1 mom. ska lämna den information till landskapsregeringen som framgår av punktlistan. Bestämmelsen genomför art. 23.4 mom. 1 i cybersäkerhetsdirektivet.

Enligt 4 mom. 1 punkten ska verksamhetsutövaren till landskapsregeringen, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande cybersäkerhetsincidenten, lämna en tidig varning som i tillämpliga fall ska ange om den betydande cybersäkerhetsincidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.

Enligt 4 mom. 2 punkten ska verksamhetsutövaren till landskapsregeringen, utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande cybersäkerhetsincidenten, lämna en incidentrapport som, i tillämpliga fall, ska uppdatera den information som avses i 1 punkten och ange en inledande bedömning av den betydande cybersäkerhetsincidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

Enligt 4 mom. 3 punkten ska verksamhetsutövaren på begäran av landskapsregeringen avge en delrapport om relevanta statusuppdateringar.

Enligt 4 mom. 4 punkten ska verksamhetsutövaren senast en månad efter inlämningen av den incidentrapport som avses i 2 punkten, avge en slutrapport som ska innehålla en detaljerad beskrivning av cybersäkerhetsincidenten, inbegripet dess allvarlighetsgrad och konsekvenser, den typ av hot eller grundorsak som sannolikt har utlöst cybersäkerhetsincidenten, tillämpade och pågående begränsande åtgärder, och, i tillämpliga fall, cybersäkerhetsincidentens gränsöverskridande verkningar.

Enligt 4 mom. 5 punkten ska verksamhetsutövaren till landskapsregeringen, i händelse av en pågående cybersäkerhetsincident vid tidpunkten för

inlämnandet av den slutrapport som avses i 4 punkten, tillhandahålla en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att den har hanterat cybersäkerhetsincidenten.

I paragrafens 5 mom. föreskrivs att en verksamhetsutövare vilken är tillhandahållare av betrodda tjänster ska, genom undantag från 4 mom. 2 punkten, när det gäller betydande cybersäkerhetsincidenter som 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. Bestämmelsen genomför art. 23.4 mom. 2 i cybersäkerhetsdirektivet.

I paragrafens 6 mom. återfinns ett förordningsbemyndigande för landskapsregeringen om utfärdande av närmare bestämmelser om formen för och innehållet i cybersäkerhetsincidentrapportering enligt 1–5 mom.

22 §. *Frivillig rapportering.* I denna paragraf föreskrivs om verksamhetsutövares frivilliga rapportering till landskapsregeringens, utöver den rapporteringsskyldighet som framgår av 21 §, av de verksamhetsutövare som uppräknas i punktlistan. Bestämmelsen genomför art. 30.1 i cybersäkerhetsdirektivet. Kommissionen får enligt art. 23.11 mom. 1 i cybersäkerhetsdirektivet anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med art. 30 i cybersäkerhetsdirektivet.

Enligt 1 punkten kan frivillig rapportering avges till landskapsregeringen av väsentliga och viktiga verksamhetsutövare, avseende på cybersäkerhetsincidenter, cyberhot och tillbud.

Enligt 2 punkten kan frivillig rapportering avges till landskapsregeringen av andra verksamhetsutövare än de som avses i 1 punkten, oberoende av om de omfattas av denna lag, avseende betydande cybersäkerhetsincidenter, cyberhot och tillbud.

23 §. *Europeiska ordningar för cybersäkerhetscertifiering.* I denna paragraf föreskrivs om väsentliga och viktiga verksamhetsutövares användning av europeiska ordningar för cybersäkerhetscertifiering. Bestämmelsen utgör nationellt handlingsutrymme, vilket utnyttjas i aktuellt fall.

I paragrafens 1 mom. föreskrivs att en väsentlig eller viktig verksamhetsutövare ska sträva efter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av verksamhetsutövaren eller har upphandlats från tredje parter, vilka är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som har antagits i enlighet med art. 49 i cybersäkerhetsakten. Bestämmelsen genomför art. 24.1 men. 1 i cybersäkerhetsdirektivet. Kommissionen kan enligt art. 24.2 cybersäkerhetsdirektivet anta delegerade genomförandeakter i enlighet med art. 38 för att komplettera direktivet genom att ange vilka kategorier av väsentliga eller viktiga verksamhetsutövare som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt art. 49 i cybersäkerhetsakten. Dessa delegerade genomförandeakter ska antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod. Innan kommissionen antar sådana delegerade akter ska den göra en konsekvensbedömning och genomföra samråd i enlighet med art. 56 i cybersäkerhetsakten. Enligt art. 24.3 i cybersäkerhetsdirektivet kan kommissionen, i fall där det inte finns en lämplig europeisk ordning för cybersäkerhetscertifiering med avseende på tillämpningen av art. 24.2, efter samråd med NIS-samarbetsgruppen och den europeiska gruppen för cybersäkerhetscertifiering, begära att Enisa utarbetar ett förslag till certifieringsordning enligt art. 48.2 i cybersäkerhetsakten.

I paragrafens 2 *mom.* föreskrivs att en väsentlig eller viktig verksamhetsutövare ska sträva efter att använda kvalificerade betrodda tjänster. Bestämmelsen genomför art. 24.1 men. 2 i cybersäkerhetsdirektivet.

24 §. *Standarder.* I denna paragraf föreskrivs att en väsentlig eller viktig verksamhetsutövare, i förekommande fall, ska sträva efter att använda tillämpliga europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i dess nätverks- och informationssystem. Bestämmelsen genomför art. 25.1 i cybersäkerhetsdirektivet. Enisa ska enligt art. 25.2 i cybersäkerhetsdirektivet i samarbete med medlemsstaterna och, när så är lämpligt, efter samråd med relevanta intressenter, utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller art. 25.1 samt för redan befintliga standarder, inklusive nationella standarder, som skulle göra det möjligt att täcka dessa områden.

6 kap. Cyberkrishanteringsmyndighet och enhet för hantering av cybersäkerhetsincidenter

25 §. *Cyberkrishanteringsmyndighet.* I denna paragraf föreskrivs att landskapsregeringen är cyberkrishanteringsmyndighet och dess ansvar i egenkap av detta.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen är cyberkrishanteringsmyndighet enligt lagen och ansvarar därmed för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Bestämmelsen genomför art. 9.1 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen ska identifiera vilka kapaciteter, tillgångar och förfaranden på Åland som kan nyttjas i händelse av en cybersäkerhetskris. Bestämmelsen genomför art. 9.3 i cybersäkerhetsdirektivet.

26 §. *Enhet för hantering av cybersäkerhetsincidenter.* I denna paragraf föreskrivs att landskapsregeringen utgör enhet för hantering av cybersäkerhetsincidenters och dess ansvar och samverkan.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen är enhet för hantering av cybersäkerhetsincidenter enligt lagen och ansvarar därmed för hanteringen av cybersäkerhetsincidenter på Åland. Bestämmelsen genomför art. 10.1 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att 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 detta ändamål ska landskapsregeringen bidra till införandet av säkra verktyg för informationsutbyte. Bestämmelsen genomför art. 10.3 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att landskapsregeringen ska samarbeta och, när det är lämpligt, utbyta relevant information om cybersäkerhet med sektoriella eller sektorsövergripande grupper av väsentliga och viktiga verksamhetsutövare. Bestämmelsen genomför art. 10.4 i cybersäkerhetsdirektivet.

I paragrafens 4 *mom.* föreskrivs att landskapsregeringen ska delta i sakkunnigbedömningar. Bestämmelsen genomför art. 10.5 i cybersäkerhetsdirektivet.

I paragrafens 5 *mom.* föreskrivs att landskapsregeringen kan upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter och utbyta relevant information med dem. Som en del av sådana samarbetsförbindelser ska ett ändamålsenligt, effektivt och säkert informationsutbyte med nationella enheter för hantering av it-säkerhetsincidenter i tredjeländer underlättas, med hjälp av relevanta protokoll för

informationsutbyte, inbegripet Trafikljusprotokollet (förkortas som *TLP* efter engelskans *Traffic Light Protocol*, vilket är ett system för att klassificera känslig information). Landskapsregeringen får utbyta relevant information med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter, inbegripet personuppgifter, i enlighet med dataskyddslagstiftningen. Bestämmelsen genomför art. 10.7 i cybersäkerhetsdirektivet.

I paragrafens 6 mom. föreskrivs att landskapsregeringen kan samarbeta med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter eller motsvarande organ, särskilt i syfte att ge dem cybersäkerhetsstöd. Bestämmelsen genomför art. 10.8 i cybersäkerhetsdirektivet.

27 §. *Krav på enheten för hantering av cybersäkerhetsincidenter och dess uppgifter.* I denna paragraf föreskrivs närmare om de krav och uppgifter som landskapsregeringen underställs i relation till sitt uppdrag att ansvara för hanteringen av cybersäkerhetsincidenter på Åland, i egenskap av enhet för hantering av cybersäkerhetsincidenter.

I paragrafens 1 mom. föreskrivs att landskapsregeringen, i egenskap av enhet för hantering av cybersäkerhetsincidenter, ska uppfylla kraven i punktlistan. Bestämmelsen genomför art. 11.1 i cybersäkerhetsdirektivet.

Enligt 1 mom. 1 punkten ska landskapsregeringen 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.

Enligt 1 mom. 2 punkten ska landskapsregeringens lokaler och de informationssystem som den använder sig av vara belägna på säkra platser.

Enligt 1 mom. 3 punkten ska landskapsregeringen ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.

Enligt 1 mom. 4 punkten ska landskapsregeringen säkerställa verksamhetens konfidentialitet och trovärdighet.

Enligt 1 mom. 5 punkten ska landskapsregeringen ha tillräckligt med personal för att säkerställa att dess tjänster är ständigt tillgängliga och ska säkerställa att personalen har fått lämplig utbildning.

Enligt 1 mom. 6 punkten ska landskapsregeringen utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i dess tjänster.

Enligt 1 mom. 7 punkten ska landskapsregeringen delta i relevanta internationella samarbetsgrupper och nätverk.

I paragrafens 2 mom. föreskrivs att landskapsregeringen, i egenskap av enhet för hantering av cybersäkerhetsincidenter, ha de uppgifter som uppräknas i punktlistan. Bestämmelsen genomför art. 11.3 mom. 1 i cybersäkerhetsdirektivet, med undantag för art. 11.3 mom. 1 led g, vilket genomförs i riket.

Enligt 1 mom. 1 punkten ska landskapsregeringen bedriva 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.

Enligt 1 mom. 2 punkten ska landskapsregeringen tillhandahålla 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,

Enligt 1 mom. 3 punkten ska landskapsregeringen vidtaga åtgärder till följd av cybersäkerhetsincidenter och, i tillämpliga fall, tillhandahållande av stöd till berörda väsentliga och viktiga verksamhetsutövare.

Enligt 1 mom. *4 punkten* ska landskapsregeringen insamla och analysera forensiska uppgifter och tillhandahålla dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

Enligt 1 mom. *5 punkten* ska landskapsregeringen, på begäran av en väsentlig eller viktig verksamhetsutövare, tillhandahålla en proaktiv skanning av verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

Enligt 1 mom. *6 punkten* ska landskapsregeringen delta i CSIRT-nätverket och ge ömsesidigt bistånd i enlighet med dess kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran.

Enligt 1 mom. *7 punkten* ska landskapsregeringen bidra till införandet av säkra verktyg för informationsutbyte enligt 25 § 2 mom.

I paragrafens *3 mom.* föreskrivs att 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. Bestämmelsen genomför art. 11.3 mom. 2 i cybersäkerhetsdirektivet.

I paragrafens *4 mom.* föreskrivs att landskapsregeringen kan, när den utför de uppgifter som avses 2 mom., prioritera särskilda uppgifter på grundval av en riskbaserad metod. Bestämmelsen genomför art. 11.3 mom. 3 i cybersäkerhetsdirektivet.

I paragrafens *5 mom.* föreskrivs att landskapsregeringen ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå lagens syfte. Bestämmelsen genomför art. 11.4 i cybersäkerhetsdirektivet.

I paragrafens *6 mom.* föreskrivs att landskapsregeringen, för att underlätta det samarbete som avses i 5 mom., ska främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller förfaranden för incidenthantering, och krishantering. Bestämmelsen genomför art. 11.5 i cybersäkerhetsdirektivet, med undantag för art. 11.5 led c, vilket genomförs i riket.

7 kap. Landskapsregeringens informationsansvar

28 §. *Arrangemang för informationsutbyte.* I denna paragraf föreskrivs om landskapsregeringens skyldighet att säkerställa informationsutbyte och underlätta arrangemang för detta om cybersäkerhet om motståndskraft mellan verksamhetsutövare och myndigheter.

I paragrafens *1 mom.* föreskrivs att landskapsregeringen ska underlätta frivilligt informationsutbyte om motståndskraft mellan kritiska verksamhetsutövare, särskilt i fråga om sekretessbelagda och känsliga uppgifter, konkurrens och skydd av personuppgifter. Bestämmelsen genomför art. 10.3 i motståndskraftsdirektivet.

I paragrafens *2 mom.* föreskrivs att landskapsregeringen ska förenkla rapportering enligt 21 och 22 §§ genom tekniska medel. Bestämmelsen genomför art. 13.6 i cybersäkerhetsdirektivet.

I paragrafens *3 mom.* föreskrivs att landskapsregeringen ska säkerställa att väsentliga eller viktiga verksamhetsutövare och, i relevanta fall, andra relevanta verksamhetsutövare som inte omfattas av denna lags tillämpningsområde, på frivillig basis har möjlighet att utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfigurationsverktyg för cybersäkerhet för att upptäcka cyberattacker, om sådant informationsutbyte syftar till att förebygga,

upptäcka, reagera på eller återhämta sig från cybersäkerhetsincidenter eller begränsa deras inverkan, och höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots förmåga att sprida sig, stödja en rad defensiva förmågor, avhjälpan av sårbarheter och delgivning av information om sårbarheter, metoder för att upptäcka och förebygga hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser, eller genom att främja forskningssamverkan om cyberhot bland offentliga och enskilda verksamhetsutövare. Bestämmelsen genomför art. 29.1 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. föreskrivs att 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 som utbyts ska genomföras med hjälp av arrangemang för informationsutbyte om cybersäkerhet. Bestämmelsen genomför art. 29.2 i cybersäkerhetsdirektivet. Enligt art. 29.5 i cybersäkerhetsdirektivet ska Enisa tillhandahålla stöd för inrättandet av de arrangemang för informationsutbyte som avses i art. 29.2 genom att utbyta bästa praxis och erbjuda vägledning.

I paragrafens 5 mom. föreskrivs att landskapsregeringen ska underlätta inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i 4 mom. Sådana arrangemang kan ange operativa aspekter, inbegripet användning av särskilda IKT-plattformar och automatiseringsverktyg, innehållet i och villkoren för de arrangemangen för informationsutbyte. Landskapsregeringen kan, i samband med fastställandet av närmare bestämmelser om myndigheters deltagande i sådana arrangemang, införa villkor för den information som 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 som ingår i den nationella strategin för cybersäkerhet. Bestämmelsen genomför art. 29.3 i cybersäkerhetsdirektivet.

I paragrafens 6 mom. föreskrivs att verksamhetsutövare ska underrätta landskapsregeringen om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet som avses i 3 mom. när de ingår i sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan. Bestämmelsen genomför art. 29.4 i cybersäkerhetsdirektivet.

29 §. *Informationsansvar vid incidenter.* I denna paragraf föreskrivs om landskapsregeringens informationsansvar vid incidenter, det vill säga hur rapportering om incidenter ska hanteras samt eventuellt vidareförmedlas.

I paragrafens 1 mom. föreskrivs att landskapsregeringen, om en incident hos en kritisk verksamhetsutövare har eller kan ha en betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater i Europeiska unionen, genom ansvarig riksmyndighet ska anmäla incidenten till kommissionen. Bestämmelsen genomför art. 15.1 mom. 2 i motståndskraftsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen, på grundval av den information som en kritisk verksamhetsutövare lämnar i sin incidentrapport, genom Finlands gemensamma kontaktpunkt ska informera gemensamma kontaktpunkter i andra medlemsstater i Europeiska unionen som 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. Bestämmelsen genomför art. 15.3 mom. 1 i motståndskraftsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen, så snart som möjligt efter incidentrapportering enligt 16 §, ska tillhandahålla berörda kritisk verksamhetsutövare relevant uppföljningsinformation, inklusive

information som skulle kunna hjälpa den att reagera ändamålsenligt på incidenten i fråga. Bestämmelsen genomför art. 15.4 men. 1 i motståndskrafts-direktivet.

I paragrafens 4 mom. föreskrivs att landskapsregeringen ska informera allmänheten om incidenter om den bedömer att det skulle ligga i allmänhetens intresse. Bestämmelsen genomför art. 15.4 men. 2 i motståndskrafts-direktivet.

30 §. *Informationsansvar vid incidenter.* I denna paragraf föreskrivs om landskapsregeringens informationsansvar vid cybersäkerhetsincidenter, det vill säga hur rapportering om cybersäkerhetsincidenter ska hanteras samt eventuellt vidareförmedlas.

I paragrafens 1 mom. föreskrivs att landskapsregeringen ska mottaga och hantera rapportering om betydande cybersäkerhetsincidenter enligt 21 § och cybersäkerhetsincidenter, cyberhot och tillbud enligt 22 §. Bestämmelsen genomför art. 13.2 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen ska informera Finlands gemensamma kontaktpunkt om de rapporter om cybersäkerhetsincidenter, cyberhot och tillbud som inkommer. Bestämmelsen genomför art. 13.3 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen, utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varning som avses i 21 § 4 mom. 1 punkten, ska lämna ett svar till en rapportrande verksamhetsutövare, inbegripet initial återkoppling om den betydande cybersäkerhetsincidenten och, på verksamhetsutövarens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder samt ytterligare tekniskt stöd. Om en betydande cybersäkerhetsincident misstänks vara av brottslig art ska landskapsregeringen även tillhandahålla vägledning om brottsanmälan. Bestämmelsen genomför art. 23.5 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. föreskrivs att landskapsregeringen kan begära att Finlands gemensamma kontaktpunkt vidarebefordrar rapporter som har mottagits i enlighet med 21 § 1 mom. till de gemensamma kontaktpunkterna i andra berörda medlemsstater i Europeiska unionen. Bestämmelsen genomför art. 23.8 i cybersäkerhetsdirektivet.

I paragrafens 5 mom. föreskrivs att landskapsregeringen vid en gränsöverskridande eller sektorsövergripande betydande cybersäkerhetsincident ska se till att Finlands gemensamma kontaktpunkt i god tid förses med relevant information som har rapporterats till myndigheten i enlighet med 21 § 4 och 5 mom. Bestämmelsen genomför art. 23.1 mom. 3 i cybersäkerhetsdirektivet.

I paragrafens 6 mom. föreskrivs att landskapsregeringen, när så är lämpligt, samt särskilt om den betydande cybersäkerhetsincidenten berör två eller flera andra medlemsstater i Europeiska unionen, utan onödigt dröjsmål genom Finlands gemensamma kontaktpunkt ska informera enheter för hantering av cybersäkerhetsincidenter i andra medlemsstater och Enisa om en betydande cybersäkerhetsincident. Informationen ska åtminstone inbegripa den som har mottagits i enlighet med 21 § 4 mom., med bevarande av verksamhetsutövares säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet, vilket ska ske i enlighet med beaktande av tillämplig unionsrätt, nationell samt åländsk rätt. Bestämmelsen genomför art. 23.6 i cybersäkerhetsdirektivet.

I paragrafens 7 mom. föreskrivs att landskapsregeringen, 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, kan efter samråd med en berörd verksamhetsutövare, informera allmänheten om en betydande

cybersäkerhetsincident eller ålägga den berörda verksamhetsutövaren att göra detta. Även enheter för hantering av cybersäkerhetsincidenter eller tillsynsmyndigheter i andra berörda medlemsstater i Europeiska unionen kan, om det är lämpligt, efter samråd med en berörd verksamhetsutövare informera allmänheten i andra medlemsstater. Bestämmelsen genomför art. 23.7 cybersäkerhetsdirektivet.

I paragrafens 8 *mom.* föreskrivs att landskapsregeringen även ska behandla frivillig rapportering enligt 22 § i enlighet med de förfaranden som anges i 3–7 *mom.*, med givande av företräde åt behandling av obligatorisk rapportering framför frivillig sådan. Bestämmelsen genomför art. 30.2 *mom.* 1 i cybersäkerhetsdirektivet.

I paragrafens 9 *mom.* föreskrivs att landskapsregeringen, vid behov, ska 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. Bestämmelsen genomför art. 30.2 *mom.* 2 i cybersäkerhetsdirektivet.

8 kap. Tillsyn och efterlevnadskontroll

31 §. *Tillsynsmyndighet.* I denna paragraf föreskrivs att landskapsregeringen är tillsynsmyndighet och om dess självständighet och oberoende i denna roll.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen är tillsynsmyndighet enligt lagen, det vill säga över såväl regleringen om cybersäkerhet som motståndskraft. Bestämmelsen genomför art. 8.1 och 8.2 i cybersäkerhetsdirektivet och art. 9.1 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen ska agera självständigt och oberoende i sin roll som tillsynsmyndighet. Bestämmelsen genomför art. 31.4 i cybersäkerhetsdirektivet.

32 §. *Stöd till samt samråd, samarbete och informationsutbyte med verksamhetsutövare om motståndskraft.* I denna paragraf föreskrivs om landskapsregeringens stöd till samt samarbete och informationsutbyte med verksamhetsutövare om motståndskraft.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen ska stödja kritiska verksamhetsutövare att stärka deras motståndskraft. Stödet kan innefatta utveckling av vägledningsmaterial och metoder, stöd till anordnande av övningar för att testa kritiska verksamhetsutövarers motståndskraft, tillhandahållande av rådgivning och utbildning för deras personal, om det är nödvändigt och motiverat av mål av ett allmänt intresse. Stödets form och omfattning utgör nationellt handlingsutrymme, vilket nyttjas fullt ut. Bestämmelsen genomför art. 10.1 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen ska samråda, samarbeta och utbyta information och god praxis om motståndskraft med kritiska verksamhetsutövare och relevanta berörda parter. Med relevanta berörda parter avses andra än myndigheter eller kritiska verksamhetsutövare som är relevanta för och berörda av arbetet med att stärka kritiska verksamhetsutövarers motståndskraft. Bestämmelsen genomför delar av art. 9.5 och art. 10.2 i motståndskraftsdirektivet.

33 §. *Myndighetssamråd och samarbete.* I denna paragraf föreskrivs om landskapsregeringens myndighetssamråd och samarbete om motståndskraft.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen, när så är lämpligt, ska samråda och samarbeta om motståndskraft med andra relevanta nationella myndigheter, inbegripet de som ansvarar för civilskydd, brotts-

bekämpning och skydd av personuppgifter. Det handlar särskilt om Ålands polismyndighet, Ålands räddningstjänst och Datainspektionen, jämte motsvarande myndigheter i riket. Bestämmelsen genomför delar av art. 9.5 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen, när så är lämpligt, ska samråda 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 som använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller fler medlemsstater, ingår i företagsstrukturer som är sammankopplade eller sammanlänkade med kritiska verksamhetsutövare i andra medlemsstater, eller har identifierats som kritiska verksamhetsutövare i en medlemsstat och tillhandahåller samhällsviktiga tjänster till eller i andra medlemsstater. Bestämmelsen genomför art. 11 i motståndskraftsdirektivet.

I paragrafens 3 *mom.* föreskrivs att landskapsregeringen genom företrädare ska delta i EU-CyCLONe, i egenskap av cyberkrishanteringsmyndighet enligt cybersäkerhetsdirektivet, samt, vid behov med säkerhetsgodkännande, i gruppen för kritiska entiteters motståndskrafts arbete, i egenskap av behörig myndighet enligt motståndskraftsdirektivet. Bestämmelsen genomför art. 16.2 i cybersäkerhetsdirektivet och art. 19.2 *mom.* 1 i motståndskraftsdirektivet.

I paragrafens 4 *mom.* föreskrivs att landskapsregeringen ska samarbeta med Finlands gemensamma kontaktpunkt, enhet för hantering av it-säkerhetsincidenter och tillsynsmyndigheter när det gäller fullgörandet av dess skyldigheter enligt denna lag och cybersäkerhetslagen. Cybersäkerhetscentret vid Transport- och kommunikationsverket är enligt cybersäkerhetslagen gemensam kontaktpunkt enligt art. 8.3, samordnande cybersäkerhetsmyndighet enligt art. 9.2 och samordnande enhet för hantering av cybersäkerhetsrisker enligt art. 12.1 i cybersäkerhetsdirektivet. Övriga rikets tillsynsmyndigheter utpekas särskilt i cybersäkerhetslagen. Bestämmelsen genomför art. 13.1 i cybersäkerhetsdirektivet.

I paragrafens 5 *mom.* föreskrivs att landskapsregeringen, 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, ska samarbeta med rikets tillsynsmyndigheter enligt cybersäkerhetslagen, brottsbekämpande myndigheter, dataskyddsmyndigheter, Transport- och kommunikationsverket och Finansinspektionen jämte andra relevanta nationella tillsynsmyndigheter enligt sektorsspecifika unionsrättsakter. Med brottsbekämpande myndigheter avses Ålands polismyndighet jämte rikets brottsbekämpande myndigheter. Med dataskyddsmyndigheter avses Datainspektionen respektive Dataombudsmannens byrå. Transport- och kommunikationsverket är enligt 42 a § lagen om stark autentisering och betrodda elektroniska tjänster (FFS 617/2009, nedan kallad *lagen om stark autentisering och betrodda elektroniska tjänster*) behörig myndighet enligt förordningen om elektronisk identifiering. Transport- och kommunikationsverket är även enligt 303 § lagen om elektronisk kommunikation behörig myndighet enligt kodexdirektivet. Transport- och kommunikationsverket är även enligt 3 § 2 och 5 punkterna luftfartslagen (FFS 864/2014, nedan kallad *luftfartslagen*) behörig myndighet enligt Europaparlamentets och rådets förordning (EG) nr 300/2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (nedan kallad *förordningen om skyddsregler*) och Europaparlamentets och rådets förordning (EU) 2018/1139 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr

2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (nedan kallad *EASA-förordningen*). Finansinspektionen är enligt 50 p § lagen om Finansinspektionen (FFS 878/2008, nedan kallad *lagen om Finansinspektionen*) behörig myndighet enligt artikel 46 och 26.9 i motståndskraftsförordningen för finanssektorn. Bestämmelsen genomför art. 13.4 i cybersäkerhetsdirektivet.

I paragrafens 6 *mom.* föreskrivs att landskapsregeringen regelbundet ska utbyta information i fråga om cybersäkerhet med Transport- och kommunikationsverket och Finansinspektionen, även när det gäller relevanta cybersäkerhetsincidenter och cyberhot. Transport- och kommunikationsverket är enligt 42 a § lagen om stark autentisering och betrodda elektroniska tjänster behörig myndighet enligt förordningen om elektronisk identifiering. Transport- och kommunikationsverket är även enligt 303 § lagen om elektronisk kommunikation behörig myndighet enligt kodexdirektivet. Transport- och kommunikationsverket är även enligt 3 § 2 och 5 punkterna luftfartslagen behörig myndighet enligt förordningen om skyddsregler och EASA-förordningen. Finansinspektionen är enligt 50 p § lagen om Finansinspektionen behörig myndighet enligt artikel 46 och 26.9 i motståndskraftsförordningen för finanssektorn. Bestämmelsen genomför art. 13.5 men. 2 i cybersäkerhetsdirektivet.

I paragrafens 7 *mom.* föreskrivs att landskapsregeringen ska samarbeta med Finansinspektionen och ska informera det tillsynsforum som har inrättats enligt artikel 32.1 i förordningen för digital operativ motståndskraft för finanssektorn när den utövar tillsyn 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. Bestämmelsen genomför art. 32.10 och 33.6 i cybersäkerhetsdirektivet.

34 §. *Rådgivande uppdrag.* I denna paragraf föreskrivs om landskapsregeringens befogenheter och skyldigheter i förhållande till rådgivande uppdrag för kritiska verksamhetsutövare.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen kan begära att kommissionen anordnar ett rådgivande uppdrag för en kritisk verksamhetsutövare, utifrån två i punktlistan angivna omständigheter.

I 1 *mom.* 1 *punkten* föreskrivs att en begäran om rådgivande uppdrag kan ske med en berörd verksamhetsutövares samtycke, i syfte att tillhandahålla rådgivning avseende uppfyllandet av dess skyldigheter enligt 4 kap. Bestämmelsen genomför art. 13.4 men. 1 i motståndskraftsdirektivet.

I 1 *mom.* 2 *punkten* föreskrivs att en begäran om rådgivande uppdrag kan ske i syfte att bedöma de åtgärder vilka en kritisk verksamhetsutövare av särskild europeisk betydelse belägen på Åland eller som tillhandahåller en samhällsviktig tjänst till eller på Åland, har vidtagit. Bestämmelsen genomför art. 18.1 och 18.2 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen, 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 betydelse samhällsviktiga tjänst tillhandahålls av en verksamhetsutövare belägen på Åland, ska tillhandahålla relevanta delar av verksamhetsutövares riskbedömning, en förteckning över relevanta åtgärder som har vidtagits för att öka verksamhetsutövares motståndskraft, och de tillsyns- och efterlevnadskontrollåtgärder som landskapsregeringen har vidtagit avseende verksamhetsutövares, inbegripet bedömningar av efterlevnad eller utfärdade förelägganden. Bestämmelsen genomför art. 18.3 i motståndskraftsdirektivet.

I paragrafens 3 *mom.* föreskrivs att landskapsregeringen ska analysera den rapport som ett rådgivande uppdrag avger för ett uppdrag enligt 1 *mom.* 2 punkten och, om så är nödvändigt, ge kommissionen råd om huruvida den berörda verksamhetsutövaren uppfyller sina skyldigheter enligt 4 kap. och, i förekommande fall, vilka åtgärder som skulle kunna vidtas för att förbättra verk-samhetsutövarens motståndskraft. Bestämmelsen genomför art. 18.4 *mom.* 2 i motståndskraftsdirektivet.

I paragrafens 4 *mom.* föreskrivs att 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 som den har vidtagit i enlighet med yttrandet. Bestämmelsen genomför art. 18.4 *mom.* 4 i motståndskraftsdirektivet.

I paragrafens 5 *mom.* föreskrivs att landskapsregeringen, vid samråd med kommissionen och i samband med anordnande av rådgivande uppdrag enligt 1 *mom.* 2 punkten, ska föreslå expertkandidater från Åland för deltagande i det rådgivande uppdraget. Bestämmelsen genomför art. 18.5 i motståndskraftsdirektivet.

I paragrafens 6 *mom.* föreskrivs att landskapsregeringen, för det fall att ett rådgivande uppdrag har ägt rum på Åland, ska informera gruppen för kritiska entiteters motståndskraft om de viktigaste resultaten av det rådgivande uppdraget och de tillvaratagna erfarenheterna, i syfte att underlätta ett ömsidigt lärande. Bestämmelsen genomför art. 18.10 i motståndskraftsdirektivet.

35 §. *Sakkunnigbedömning.* I denna paragraf föreskrivs om landskapsregeringens befogenheter och skyldigheter i förhållande till en sakkunnigbedömning.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen, på grundval av NIS-samarbetsgruppens fast-ställda metoder, kan utse cybersäkerhetsexperter för deltagande vid en sakkunnigbedömning. Bestämmelsen genomför art. 19.1 och 19.2 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen ska informera kommissionen, Enisa, NIS-samarbetsgruppen och behöriga myndigheter i andra medlemsstater i Europeiska unionen om alla risker för intressekonflikter som rör dess utsedda cybersäkerhetsexperter innan en sakkunnigbedömning inleds. Bestämmelsen genomför art. 19.8 *men.* 1 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs om särskilda föreskrifter för de fall vilka Åland är föremål för en sakkunnigbedömning, enligt punktlistan.

I paragrafens 3 *mom.* 1 *punkten* föreskrivs att landskapsregeringen kan identifiera särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär. Bestämmelsen genomför art. 19.3 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* 2 *punkten* föreskrivs att landskapsregeringen ska, innan en sakkunnigbedömning inleds informera behöriga myndigheter i deltagande medlemsstater om omfattningen av sakkunnigbedömningen, inbegripet de särskilda frågor som har identifierats enligt 1 *punkten*. Bestämmelsen genomför art. 19.4 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* 3 *punkten* föreskrivs att landskapsregeringen kan, innan en sakkunnigbedömning inleds, genomföra en självuppskattning av de granskade aspekterna och tillhandahålla den till de utsedda cybersäkerhetsexperterna. Bestämmelsen genomför art. 19.5 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* 4 *punkten* föreskrivs att landskapsregeringen ska förse utsedda cybersäkerhetsexperter med den information som krävs för sakkunnigbedömningen, utan att det påverkar skyddet av sekretessbelagda

uppgifter samt skyddet av väsentliga allmänna intressen. Bestämmelsen genomför art. 19.6 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. *5 punkten* föreskrivs att landskapsregeringen kan, av vederbörligen motiverade skäl, invända mot utnämningen av en särskild cybersäkerhetsexpert, vilka ska meddelas den andra medlemsstatens utseende behöriga myndighet. Bestämmelsen genomför art. 19.8 men. 2 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. *6 punkten* föreskrivs att landskapsregeringen kan lämna synpunkter på ett utkast till en cybersäkerhetsexperts rapport som berör Åland, vilka ska bifogas till rapporten. Bestämmelsen genomför delar av art. 19.9 men. 2 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. *7 punkten* föreskrivs att landskapsregeringen kan besluta att offentliggöra sin rapport eller en redigerad version av den. Bestämmelsen genomför 19.9 men. 5 i cybersäkerhetsdirektivet.

36 §. *Tillsyn och efterlevnadskontroll av kritiska verksamhetsutövare.* I denna paragraf föreskrivs om landskapsregeringens befogenheter att vidta tillsyns- och efterlevnadskontrollåtgärder gentemot kritiska verksamhetsutövare, i syfte att säkerställa deras efterlevnad av lagens bestämmelser om motståndskraft.

I paragrafens *1 mom.* föreskrivs att landskapsregeringen vid tillsyn av kritiska verksamhetsutövare ska ha befogenhet att vidta tillsynsåtgärder, enligt punktlistan.

I paragrafens 1 mom. *1 punkten* föreskrivs att landskapsregeringen kan 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. Bestämmelsen genomför art. 21.1 led a i motståndskraftsdirektivet.

I paragrafens 1 mom. *2 punkten* föreskrivs att landskapsregeringen kan utföra eller beställa säkerhetsrevisioner. Bestämmelsen genomför art. 21.1 led b i motståndskraftsdirektivet.

I paragrafens 1 mom. *3 punkten* föreskrivs att landskapsregeringen kan 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, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad revisor som har valts av verksamhetsutövaren och som har utförts på verksamhetsutövarens bekostnad. Av föreläggandet ska syftet och en närmare redogörelse för vilken information som begärs framgå. Bestämmelsen genomför art. 21.2 i motståndskraftsdirektivet.

I paragrafens *2 mom.* föreskrivs att vid konstaterade brister eller överträdelse av skyldigheter enligt 4 kap. vid efterlevnadskontroll av en kritisk verksamhetsutövare kan, med hänsyn tagen till överträdelsens allvarighet, 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. Vid utfärdandet av föreläggandet ska landskapsregeringen framför allt ta hänsyn till hur allvarlig överträdelsen har varit. Ett åtgärdsföreläggande enligt momentet påverkar inte möjligheten att ålägga en verksamhetsutövare administrativa påföljdssavgifter. Bestämmelsen genomför art. 21.3 i motståndskraftsdirektivet.

37 §. *Allmän inriktning på tillsyn och efterlevnadskontroll av väsentliga eller viktiga verksamhetsutövare.* I denna paragraf föreskrivs den allmänna inriktning som landskapsregeringens tillsyn och efterlevnadskontroll av väsentliga och viktiga verksamhetsutövare ska ha.

I paragrafens *1 mom.* föreskrivs att landskapsregeringen på ett ändamålsenligt sätt ska övervaka och vidta de tillsyns- och

efterlevnadskontrollåtgärder som krävs för att säkerställa att väsentliga och viktiga verksamhetsutövare efterlever denna lags bestämmelser om cybersäkerhet. Bestämmelsen genomför art. 31.1 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen kan prioritera tillsyn och fastställa tillsynsmetoder vilka möjliggör att vid utövandet av dess tillsynsuppgifter prioritera uppgifter enligt en riskbaserad bedömning. Bestämmelsen genomför art. 31.2 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen ska ha ett nära samarbete med Datainspektionen och Dataombudsmannens byrå när den behandlar cybersäkerhetsincidenter vid väsentliga eller viktiga verksamhetsutövare som medför personuppgiftsincidenter, utan att detta påverkar Datainspektionens eller Dataombudsmannens byrås befogenheter och uppgifter enligt den allmänna dataskyddsförordningen. Bestämmelsen genomför art. 31.3 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. föreskrivs att 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 omständigheterna i punktlistan. Bestämmelsen genomför art. 32.1, delar av 32.7, delar av 33.1 och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. 1 punkten föreskrivs att landskapsregeringen vid vidtagande av efterlevnadskontrollåtgärder ska ta hänsyn till överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, varav upprepade överträdelser, underlåtenhet att rapportera om eller avhjälpa betydande cybersäkerhetsincidenter, underlåtenhet att avhjälpa brister enligt bindande instruktioner eller föreläggande från landskapsregeringen, förhindrande av revisioner eller övervakningsverksamhet, vilka landskapsregeringen har beordrat efter det att en överträdelse har konstaterats, och tillhandahållande av falsk eller grovt felaktig information, i fråga om åtgärder för cybersäkerhet eller rapporteringsskyldigheter, alltid ska anses utgöra en allvarlig överträdelse. Bestämmelsen genomför art. 32.7 led a och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. 2-8 punkterna föreskrivs att landskapsregeringen vid vidtagande av efterlevnadskontrollåtgärder även ska ta hänsyn till överträdelsens varaktighet, eventuella tidigare relevanta överträdelser av den berörda verksamhetsutövaren, den materiella eller immateriella skada som har uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs, uppsåt eller oaktsamhet av den som har gjort sig skyldig till överträdelsen, de skadeförebyggande och begränsande åtgärder som verksamhetsutövaren har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan, efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer och i vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med landskapsregeringen. Bestämmelserna genomför art. 32.7 led b-h och delar av 33.5 i cybersäkerhetsdirektivet.

I paragrafens 5 mom. föreskrivs att landskapsregeringen utförligt ska 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. Bestämmelsen genomför art. 32.8 och delar av 33.5 i cybersäkerhetsdirektivet.

38 §. *Tillsyn och efterlevnadskontroll av väsentliga verksamhetsutövare.* I denna paragraf föreskrivs om landskapsregeringens befogenheter att vidta tillsyns- och efterlevnadskontrollåtgärder gentemot väsentliga

verksamhetsutövare, i syfte att säkerställa deras efterlevnad av lagens bestämmelser om cybersäkerhet.

I paragrafens 1 mom. föreskrivs att landskapsregeringen vid tillsyn av väsentliga verksamhetsutövare ska ha befogenhet att vidta tillsynsåtgärder, enligt punktlistan.

I paragrafens 1 mom. 1 punkten föreskrivs att landskapsregeringen kan genomföra inspektioner på plats av lokaler och tillsyn på distans av vidtagna åtgärder för cybersäkerhet, inklusive slumpvisa kontroller som utförs av utbildad personal. Bestämmelsen genomför art. 32.2 mom. 1 led a i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 2 punkten föreskrivs att landskapsregeringen kan utföra eller beställa regelbundna och riktade säkerhetsrevisioner, vilka utförs av ett oberoende organ eller av landskapsregeringen. De riktade säkerhetsrevisioner som avses i 2 punkten ska baseras på riskbedömningar som utförs av landskapsregeringen eller den granskade verksamhetsutövaren, eller på annan tillgänglig riskrelaterad information. Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för landskapsregeringen. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade verksamhetsutövaren, utom i vederbörligen motiverade fall, när landskapsregeringen har beslutat något annat. Bestämmelsen genomför art. 32.2 mom. 1 led b och 32.2 mom. 2 och 3 i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 3 punkten föreskrivs att landskapsregeringen kan utföra ad hoc-revisioner, inbegripet när detta är motiverat på grund av en betydande cybersäkerhetsincident eller av en väsentlig verksamhetsutövares överträdelse av denna lag, och säkerhetsskanningar, på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier, vid behov i samarbete med verksamhetsutövaren. Bestämmelsen genomför delar av art. 32.2 mom. 1 led c–d i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 4 punkten föreskrivs att landskapsregeringen kan förelägga verksamhetsutövaren att, inom en rimlig tidsfrist, lämna nödvändig information för att landskapsregeringen ska kunna bedöma vidtagna åtgärder för cybersäkerhet, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till landskapsregeringen, lämna tillgång till nödvändiga uppgifter, handlingar och information för att landskapsregeringen ska kunna utföra sina tillsynsuppgifter, och bevis på genomförandet av cybersäkerhetsstrategier, exempelvis resultaten av säkerhetsrevisioner som har utförts av en kvalificerad revisor och respektive underliggande bevis. Av föreläggandet ska syftet och en närmare redogörelse för vilken information som begärs framgå. Bestämmelsen genomför art. 32.2 mom. 1 led e–g och 32.3 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen vid efterlevnadskontroll av väsentliga verksamhetsutövare ska ha befogenhet att vidta efterlevnadskontrollsåtgärder, enligt punktlistan.

I paragrafens 2 mom. 1 punkten föreskrivs att landskapsregeringen kan utfärda en skriftlig varning till verksamhetsutövaren. Bestämmelsen genomför art. 32.4 led a i cybersäkerhetsdirektivet.

I paragrafens 2 mom. 2 punkten föreskrivs att landskapsregeringen kan anta bindande instruktioner, även om vilka åtgärder som krävs för att förebygga eller avhjälpa en cybersäkerhetsincident, samt tidsgränser för genomförandet av sådana åtgärder och för rapporteringen om deras genomförande, eller förelägga verksamhetsutövaren att avhjälpa konstaterade brister eller överträdelser. Bestämmelsen genomför art. 32.4 led b i cybersäkerhetsdirektivet.

I paragrafens 2 mom. 3 punkten föreskrivs att landskapsregeringen kan ålägga verksamhetsutövaren att upphöra med handlingssätt som utgör en

överträdelse att avstå ifrån att upprepa dessa. Bestämmelsen genomför art. 32.4 led c i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *4 punkten* föreskrivs att landskapsregeringen kan ålägga verksamhetsutövaren att säkerställa att nödvändiga åtgärder för cybersäkerhet vidtas eller rapporteringsskyldigheter fullföljs, på ett närmare angivet sätt och inom en angiven tidsperiod. Bestämmelsen genomför art. 32.4 led d i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *5 punkten* föreskrivs att landskapsregeringen kan ålägga verksamhetsutövaren att, inom en rimlig tidsfrist, genomföra de rekommendationer som har lämnats till följd av en säkerhetsrevision. Bestämmelsen genomför art. 32.4 led f i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *6 punkten* föreskrivs att landskapsregeringen kan ålägga verksamhetsutövaren att informera de fysiska eller juridiska personer, till vilka den tillhandahåller tjänster eller utför verksamheter, vilka potentiellt kan beröras av ett betydande cyberhot om hotets karaktär och om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa kan vidta som svar på hotet. Bestämmelsen genomför art. 32.4 led e i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *7 punkten* föreskrivs att landskapsregeringen kan ålägga en berörd verksamhetsutövare att offentliggöra aspekter av överträdelser av denna lag på ett närmare sätt. Bestämmelsen genomför art. 32.4 led h i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *8 punkten* föreskrivs att landskapsregeringen kan utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att en berörd verksamhetsutövare efterlever skyldigheterna för väsentliga verksamhetsutövare enligt denna lag. Bestämmelsen genomför art. 32.4 led g i cybersäkerhetsdirektivet.

I paragrafens 2 mom. *9 punkten* föreskrivs att landskapsregeringen, utöver någon av de åtgärder som avses i 1–8 punkterna, kan påföra verksamhetsutövaren administrativa påföljdssavgifter. Bestämmelsen genomför art. 32.4 led i i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen, om efterlevnadskontrollåtgärder enligt 2 mom. 1–5 punkterna är ineffektiva, kan fastställa en tidsfrist inom vilken verksamhetsutövaren ska ha vidtagit nödvändiga åtgärder för att avhjälpa konstaterade brister eller uppfylla landskapsregeringens krav. Bestämmelsen genomför art. 32.5 mom. 1 men. 1 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. föreskrivs att landskapsregeringen, om en enskild väsentlig verksamhetsutövare underlåter att vidta förelagda åtgärder inom en fastställd tidsfrist, fram till dess att föreläggandet har efterföljts kan vidta följande ytterligare efterlevnadskontrollåtgärder, enligt punktlistan. Tillfälliga upphävanden eller verksamhetsförbud i enlighet med detta moment ska därmed tillämpas endast till dess att den berörda verksamhetsutövaren vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfyller de ålägganden från landskapsregeringen som gav upphov till efterlevnadskontrollåtgärden. Bestämmelsen genomför art. 32.5 mom. 1 men. 2, mom. 2 men. 1 och mom. 3 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. *1 punkten* föreskrivs att landskapsregeringen kan besluta att viss tid, dock högst fem år, upphäva verksamhetsutövarens koncession, tillstånd eller certifiering, för en del av eller samtliga relevanta tjänster eller verksamheter. Bestämmelsen genomför art. 32.5 mom. 1 men. 2 led a i cybersäkerhetsdirektivet.

I paragrafens 4 mom. *2 punkten* föreskrivs att landskapsregeringen kan besluta att 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. Bestämmelsen genomför art. 32.5 mom. 1 men. 2 led b i cybersäkerhetsdirektivet.

39 §. *Tillsyn och efterlevnadskontroll av viktiga verksamhetsutövare.* I denna paragraf föreskrivs om landskapsregeringens befogenheter att vidta tillsyns- och efterlevnadskontrollåtgärder gentemot viktiga verksamhetsutövare, i syfte att säkerställa deras efterlevnad av lagens bestämmelser om cybersäkerhet.

I paragrafens 1 mom. föreskrivs att landskapsregeringen, när den får bevis för, indikationer på eller information om att en viktig verksamhetsutövare underlåter att fullgöra sina skyldigheter enligt denna lag, vid behov ska vidta tillsyns- och efterlevnadskontrollåtgärder i efterhand. Bestämmelsen genomför delar av art. 33.1 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen vid tillsyn av en viktig verksamhetsutövare kan vidta följande tillsynsåtgärder, vidta motsvarande tillsynsåtgärder enligt 38 § 1 mom., med undantag för regelbundna säkerhetsrevisioner och ad hoc-revisioner enligt 2 och 3 punkterna. Bestämmelsen genomför art. 33.2 och 33.3 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen vid konstaterade brister eller överträdelser vid efterlevnadskontroll av en viktig verksamhetsutövare kan vidta motsvarande efterlevnadskontrollåtgärder enligt 38 § 2 mom., med undantag för utseende av en övervakningsansvarig enligt 8 punkten. Bestämmelsen genomför art. 33.4 i cybersäkerhetsdirektivet.

40 §. *Rätt att få information.* I denna paragraf föreskrivs om landskapsregeringens rätt att få information samt att vidareförmedla denna till Finlands gemensamma kontaktpunkter och tillsynsmyndigheter enligt rikets direktivgenomföranden.

Enligt paragrafens 1 mom. har landskapsregeringen 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. Genom bestämmelsen genomförs delar av art. 32.2 mom. 1 led d–g och art. 33.2 mom. 1 led c–f i cybersäkerhetsdirektivet och art. 21.2 mom. 1 i motståndskraftsdirektivet.

Enligt paragrafens 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 som landskapsregeringen har begärt och avgiftsfritt. Genom bestämmelsen genomförs delar av art. 32.3 och 33.3 i cybersäkerhetsdirektivet och art. 21.2 mom. 2 i motståndskraftsdirektivet.

Enligt paragrafens 3 mom. har landskapsregeringen trots sekretessbestämmelser och andra begränsningar rätt att till Finlands gemensamma kontaktpunkter, enhet för hantering av it-säkerhetsincidenter och 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. Genom bestämmelsen möjliggörs vidareförmedling av information och samarbete med ansvariga riksmyndigheter, vilket cybersäkerhets- och motståndskraftsdirektiven förutsätter för ett korrekt genomförande, bland annat genom att ansvariga riksmyndigheter som den gemensamma kontaktpunkten förutsätts kunna vidareförmedla viss information till exempelvis kommissionen, samarbetsgrupper, europeiska organ och andra medlemsstaters gemensamma kontaktpunkter och myndigheter.

41 §. *Inspektioner.* I denna paragraf föreskrivs närmare om landskapsregeringens inspektioner av kritiska verksamhetsutövare enligt 36 § 1 mom. 1 punkten, väsentliga verksamhetsutövare enligt 38 § 1 mom. 1 punkten och viktiga verksamhetsutövare enligt 39 § 2 mom. Genom paragrafen

genomförs art. 32.2 mom. 1 led a och delvis led d, art. 32.4 led g samt art. 33.2 mom. 1 led a och delvis led c i cybersäkerhetsdirektivet och art. 21.1 led a i motståndskraftsdirektivet.

Enligt paragrafens 1 mom. kan landskapsregeringen 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.

Enligt paragrafens 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 dock inte ske i utrymmen vilka är avsedda för boende av permanent natur.

Enligt paragrafens 3 mom. har landskapsregeringen 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.

Enligt paragrafens 4 mom. kan landskapsregeringen, 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 som förrättar inspektionen och som deltar i denna ska ha sådan utbildning och erfarenhet som 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).

Enligt paragrafens 5 mom. tillämpas i övrigt på förfarandet vid inspektioner vad som i 34 § i förvaltningslagen (2008:9) för landskapet Åland föreskrivs om inspektion.

42 §. *Internationell handräckning.* I denna paragraf föreskrivs om landskapsregeringens befogenheter och skyldigheter avseende internationell handräckning i förhållande till tillsynsmyndigheter i andra medlemsstater i Europeiska unionen avseende gränsöverskridande väsentliga eller viktiga verksamhetsutövare. Till följd av behörighetsfördelningen mellan landskapet och riket måste kontakterna i praktiken skötas genom Finlands gemensamma kontaktpunkt.

I paragrafens 1 mom. föreskrivs att landskapsregeringen ska vid tillsyn och efterlevnadskontroll av en gränsöverskridande väsentlig eller viktig verksamhetsutövare, det vill säga en verksamhetsutövare vilken tillhandahåller tjänster i mer än en medlemsstat i Europeiska unionen, eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater, vid behov ska samarbeta med och bistå andra berörda medlemsstaters tillsynsmyndigheter, åtminstone i den omfattning som punktlistan föreskriver. Bestämmelsen genomför art. 37.1 mom. 1 i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 1 punkten föreskrivs att landskapsregeringen genom Finlands gemensamma kontaktpunkt ska informera och samråda om de tillsyns- och efterlevnadskontrollåtgärder vilka den har vidtagit. Bestämmelsen genomför art. 37.1 mom. 1 led a i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 2 punkten föreskrivs att landskapsregeringen kan begära att tillsyns- eller efterlevnadskontrollåtgärder vidtas. Bestämmelsen genomför art. 37.1 mom. 1 led b i cybersäkerhetsdirektivet.

I paragrafens 1 mom. 3 punkten föreskrivs att landskapsregeringen, efter mottagande av en motiverad begäran därom, ska tillhandahålla bistånd, i proportion till sina egna resurser, i syfte att tillsyns- eller efterlevnadskontrollåtgärder ska kunna genomföras på ett ändamålsenligt, effektivt och konsekvent sätt, i form av information eller tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. Bestämmelsen genomför art. 37.1 mom. 1 led c och mom. 2 men. 1 i cybersäkerhetsdirektivet.

I paragrafens 2 mom. föreskrivs att landskapsregeringen inte kan avslå en begäran om bistånd enligt 1 mom. 3 punkten som riktas till den, med undantag för fall i vilka landskapsregeringen inte är behörig att tillhandahålla det begärda biståndet, det begärda biståndet inte står i proportion till landskapsregeringens tillsynsuppgifter, eller begäran avser information eller innefattar åtgärder som, om den lämnas ut eller de vidtas, skulle strida mot ett väsentligt nationellt säkerhetsintresse, allmän säkerhet eller försvar. Bestämmelsen genomför art. 37.1 mom. 2 men. 2 i cybersäkerhetsdirektivet.

I paragrafens 3 mom. föreskrivs att landskapsregeringen, innan den avslår en begäran om bistånd enligt 1 mom. 3 punkten, genom Finlands gemensamma kontaktpunkt ska samråda med övriga berörda tillsynsmyndigheter samt, på begäran av en av dem, även med kommissionen och Enisa. Bestämmelsen genomför art. 37.1 mom. 2 men 3 i cybersäkerhetsdirektivet.

I paragrafens 4 mom. föreskrivs att landskapsregeringen, när så är lämpligt, i samförstånd tillsammans med andra tillsynsmyndigheter kan vidta gemensamma tillsynsåtgärder. Bestämmelsen genomför art. 37.2 i cybersäkerhetsdirektivet.

43 §. *Anmälan av cybersäkerhetsöverträdelser vilka innebär personuppgiftsincidenter.* I denna paragraf föreskrivs om landskapsregeringens skyldighet att anmäla överträdelser av lagens skyldigheter för väsentliga eller viktiga verksamhetsutövare om cybersäkerhet enligt 5 kap. vilka även utgör personuppgiftsincidenter.

I paragrafens 1 mom. föreskrivs att landskapsregeringen, 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, enligt definitionen i art. 4.12, vilken ska anmälas enligt art. 33 i den förordningen, utan onödigt dröjsmål ska anmäla saken till Datainspektionen eller, i tillämpliga fall, Dataombudsmannens byrå. På Åland är Datainspektionen enligt 14 § landskapslag (2019:9) om dataskydd inom landskaps- och kommunalförvaltningen tillsynsmyndighet enligt lagen och den allmänna dataskyddsförordningen över vid landskapets myndigheter, kommunala myndigheter och till Ålands lagting ansluten förvaltning samt vid landskapets affärsverk då de sköter offentliga förvaltningsuppgifter samt på andra juridiska och fysiska personer då de genom landskapslag eller med stöd av landskapslag sköter offentliga förvaltningsuppgifter, dock inte vid Ålands polismyndighet. Enligt 1 § landskapslag (2019:74) om tillämpning på Åland av riksförfattningar om dataskydd är dataskyddslagen (FFS 1050/2018, nedan kallad *dataskyddslagen*), lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (FFS 1054/2018) samt lagen om behandling av personuppgifter i polisens verksamhet (FFS 616/2019) tillämpliga på Åland med de avvikelser som anges i lagen. Enligt 4 § samma lag fungerar Datainspektionen som tillsynsmyndighet enligt den allmänna dataskyddsförordningen och ansvarar i stället för Dataombudsmannens byrå för den tillsyn som avses i 8 § i dataskyddslagen och

45 § i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten. Dataombudsmannens byrå är dock till följd av rikets behörighet över dataskyddet hos privata verksamhetsutövare fortsatt tillsynsmyndighet över dessa enligt den allmänna dataskyddsförordningen enligt 8 § dataskyddslagen. Bestämmelsen genomför art. 35.1 i cybersäkerhetsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen, om den behöriga tillsynsmyndigheten enligt den allmänna dataskyddsförordningen är etablerad i en annan medlemsstat i Europeiska unionen, ska anmäla saken till Datainspektionen eller, i tillämpliga fall, Dataombudsmannens byrå. Bestämmelsen reglerar att landskapsregeringen inte ska vända sig direkt till behöriga tillsynsmyndigheter enligt den allmänna dataskyddsförordningen i andra medlemsstater, utan alltid vänder sig till Ålands eller rikets dito, utifrån deras ansvarsfördelning kopplad till behörigheten. För närmare redogörelse av respektive myndighets ansvarsfördelning, se detaljmotiveringen till 1 *mom.* ovan. Bestämmelsen genomför art. 35.3 i cybersäkerhetsdirektivet.

44 §. *Vite samt hot om tvångsutförande och avbrytande.* I denna paragraf föreskrivs att landskapsregeringen kan förena ett beslut som den har fattat med stöd av lagen 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, vilken med vissa ändringar tillämpliggör viteslagen (FFS 1113/1990) på Åland, tillämpas. Ett beslut kan bara förenas med ett hot om avbrytande om det avser en väsentlig eller viktig verksamhetsutövare som inte samtidigt utgör en kritisk verksamhetsutövares samhällsviktiga tjänster, vars avbrott i tillhandahållandet lagen syftar till att skydda. Bestämmelsen genomför art. 34.6 i cybersäkerhetsdirektivet och art. 22 i motståndskraftsdirektivet.

45 §. *Administrativ påföljdsavgift.* I denna paragraf föreskrivs om landskapsregeringens möjligheter och villkor för att påföra en verksamhetsutövare en administrativ påföljdsavgift till följd av att den har brutit mot lagens skyldigheter.

I paragrafens 1 *mom.* föreskrivs att landskapsregeringen genom beslut kan ålägga en enskild verksamhetsutövare, vilken uppsåtligen eller av grov oaktsamhet bryter mot dess skyldigheter enligt denna lag, att erlægga en administrativ påföljdsavgift. En administrativa påföljdsavgift ska påföras utöver någon annan efterlevnadskontrollåtgärd och utesluter därmed inte andra åtgärder. Bestämmelsen genomför art. 34.1, 34.2 och 36 i cybersäkerhetsdirektivet och art. 22 i motståndskraftsdirektivet.

I paragrafens 2 *mom.* föreskrivs att landskapsregeringen i varje enskilt fall ska, 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. Bestämmelsen genomför art. 34.3 i cybersäkerhetsdirektivet.

I paragrafens 3 *mom.* föreskrivs att en administrativ sanktionsavgift vilken påförs en kritisk verksamhetsutövare ska som minst uppgå till minst 2 000 och som högst till 20 000 euro. Beloppen är harmoniserade med försummelseavgiften enligt rikets motståndskraftslag. Bestämmelsen genomför art. 22 i motståndskraftsdirektivet.

I paragrafens 4 *mom.* föreskrivs att en administrativ sanktionsavgift 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 som den väsentliga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst. Bestämmelsen genomför art. 34.4 i cybersäkerhetsdirektivet.

I paragrafens 5 mom. föreskrivs att en administrativ sanktionsavgift 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 som den viktiga verksamhetsutövaren tillhör, beroende på vilken siffra som är högst. Bestämmelsen genomför art. 34.5 i cybersäkerhetsdirektivet.

I paragrafens 5 mom. föreskrivs att landskapsregeringen, om påföljdskollegiet har beslutat att påföra en verksamhetsutövare en administrativ sanktionsavgift enligt art. 83 i den allmänna dataskyddsförordningen, inte ska påföra en väsentlig eller viktig verksamhetsutövare en administrativ påföljdsavgift för en överträdelse enligt 41 § och som följer av samma gärning. En administrativ sanktionsavgift enligt art. 58.2 i jämte 83 i den allmänna dataskyddsförordningen jämte 24 § dataskyddslagen och 4 och 5 §§ landskapslagen om tillämpning på Åland av riskförfattningar om dataskydd, vilken tillämpliggör 24 § dataskyddslagen om administrativa påföljdsavgifter. Landskapsregeringen får emellertid fortsatt ålägga verksamhetsutövaren övriga efterlevnadskontrollåtgärder som föreskrivs i 38 § 2 och 3 mom. samt 39 3 mom. Bestämmelsen genomför art. 35.2 i cybersäkerhetsdirektivet.

46 §. *Verkställighet av påföljdsavgift.* Bestämmelsen innehåller en informativ hänvisning om att bestämmelser om verkställighet av påföljdsavgifter återfinns i lagen om verkställighet av böter (FFS 672/2002) samt föreskriver att en påföljdsavgift preskriberas när fem år har förflutit från den dag då det lagakraftvunna beslutet om avgiften meddelades. Bestämmelsen genomför art. 36 i cybersäkerhetsdirektivet och art. 22 i motståndskraftsdirektivet.

47 §. *Ändringssökande.* Denna paragraf innehåller en informativ hänvisning om en berörd verksamhetsutövares rättsskyddsförutsättning genom ändringssökande, när den har blivit föremål för landskapsregeringens beslut enligt lagen. En berörd verksamhetsutövare som inte är nöjd med landskapsregeringens beslut får enligt 25 § 2 mom. självstyrelselagen söka ändring genom besvär hos Högsta förvaltningsdomstolen, på det sätt som föreskrivs i lagen om rättegång i förvaltningsärenden (FFS 808/2019). Bestämmelsen genomför tillsammans med självstyrelselagen och rikets lagstiftning delar av art. 32.5 mom. 2 men. 2 i cybersäkerhetsdirektivet och delar av art. 21.4 i motståndskraftsdirektivet.

48 §. *Ikraftträdande.* I denna paragraf föreskrivs att lagen ska träda i kraft den

Lagtext

Landskapsregeringen föreslår att följande lagar antas.

L A N D S K A P S L A G 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 informationssystemens 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 verksamhetsutövers nätverks- och informationssystem eller användarna av verksamhetsutövers 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 vilka 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 vilken 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 verksamhetsutövers 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, 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 har inrättats 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 inrättats 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 motståndskraftdirektivet.

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 systemrisk, 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. alltså 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, betrodna tjänster, allmänt tillgängliga elektroniska kommunikationstjänster, utlokaliserade drifttjänster, 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 motståndskraftdirektivet 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 senast den 17 april 2025, samt därefter när så är nödvändigt, identifiera andra än redan 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 §

Uppgifter om verksamhetsutövare för förteckning

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 senast den 17 januari 2025 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 senast den 17 juli 2026 till ansvarig riksmyndighet överlämna samtliga de uppgifter vilka den behöver för att upprätta en förteckning över kritiska verksamhetsutövare och fullgöra sina övriga uppgifter som gemensam kontaktpunkt enligt lagen om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft.

Landskapsregeringen ska senast den 17 april 2025 till ansvarig riksmyndighet överlämna samtliga de uppgifter vilka den behöver för att upprätta en förteckning över väsentliga och viktiga verksamhetsutövare och fullgöra sina övriga uppgifter som gemensam kontaktpunkt enligt cybersäkerhetslagen.

Landskapsregeringen ska genom ansvarig riksmyndighet senast den 17 april 2025 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 genom ansvarig riksmyndighet fram till den 17 april 2025 och på begäran av kommissionen meddela namnen på de väsentliga och viktiga verksamhetsutövare vilka avses i 3 mom. 2 punkten.

Landskapsregeringen ska genom ansvarig riksmyndighet, utan onödigt dröjsmål, underrätta kommissionen om identiteten på kritiska verksamhetsutövare vilka kan utgöra kritiska verksamhetsutövare av europeisk betydelse samt om den information vilken verksamhetsutövaren har tillhandahållit om dess tillhandahållande av samhällsviktiga tjänster vilka är av betydelse för denna bedömning. Vid efterföljande samråd med kommissionen ska landskapsregeringen genom ansvarig riksmyndighet informera kommissionen om den bedömer att de tjänster vilka en kritisk verksamhetsutövare tillhandahåller på Åland är samhällsviktiga tjänster.

4 kap. Kritiska verksamhetsutövers 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 motståndskraftdirektivet 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 hantierat 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 genom rikets ansvariga myndighet upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av cybersäkerhetsincidenter och utbyta relevant information med dem.

Landskapsregeringen kan genom rikets ansvariga myndighet 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 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 genom ansvarig riksmyndighet, 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 kritisk verksamhetsutövare 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 rapporterade 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 rapporterad 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 nationella myndigheter.

Landskapsregeringen ska genom ansvarig riksmyndighet, 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, enhet för hantering av it-säkerhetsincidenter och tillsynsmyndigheter när det gäller fullgörandet av dess 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 Finlands tillsynsmyndigheter, brottsbekämpande myndigheter, dataskyddsmyndigheter, Transport- och kommunikationsverket och Finansinspektionen jämte andra

relevanta nationella tillsynsmyndigheter 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.

34 §

Rådgivande uppdrag

Landskapsregeringen kan genom ansvarig riksmyndighet 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, genom ansvarig riksmyndighet 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, genom ansvarig riksmyndighet 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 genom ansvarig riksmyndighet 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 genom ansvarig riksmyndighet, 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 genom ansvarig riksmyndighet, 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 genom ansvarig riksmyndighet 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 genom ansvarig riksmyndighet, 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 genom ansvarig riksmyndighet, av vederbörligen motiverade skäl, invända mot utnämningen av en särskild cybersäkerhetsexpert, vilket ska meddelas den andra medlemsstatens utseende behöriga myndighet,

6) landskapsregeringen kan genom ansvarig riksmyndighet 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 efterlevnadskontrollåtgärder 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 avhjälpan 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 till Finlands gemensamma kontaktpunkter, enhet för hantering av it-säkerhetsincidenter och 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 gränsoverskridande 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 erlagga en administrativ påföljdsavgift.

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 minst 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 §

Ändringsökande

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

9 kap.

Särskilda bestämmelser

48 §

Ikraftträdande

Denna lag träder i kraft den

Mariehamn den

L a n t r å d

Föredragande minister