DANSKE REVISORER FSR

Digitaliseringsministeriet
Stormgade 2-6
1470 København K

Att.: Hannah-Jean Gardner og Magnus Møller Elkjær
Pr. e-mail: hangar@digmin.dk; magelk@digmin.dk

2. juni 2026

FSR – danske revisorer

Børsgade 4, 4. sal
DK - 1215 København K

Telefon +45 7225 5703
fsr@fsr.dk
www.fsr.dk

CVR. 55 09 72 16
Danske Bank
Reg. 9541
Konto nr. 2500102295

FSR – danske revisorers høringssvar: Europa-Kommissionens forslag til forordning "Authorisation of systems providing mobile satellite services (MSS)"

RESUMÉ (max 10 linjer)
FSR – danske revisorer støtter, at der stilles krav om dokumentation og løbende monitorering i forbindelse med Europa-Kommissionens forslag om autorisation af mobile satellittjenester (MSS). Vi foreslår, at den årlige statusrapport understøttes af en uafhængig erklæring, fx efter ISAE 3000, for at sikre troværdighed og dokumenteret fremdrift. FSR – danske revisorer finder ikke, at det er tilstrækkeligt beskrevet, hvordan krav om cybersikkerhed, netværksbrug og databeskyttelse skal kontrolleres og rapporteres i praksis. Vi foreslår derfor en mere ensartet verificeringsmodel på tværs af EU, som både kan styrke compliance og reducere administrative omkostninger.

FSR - danske revisorer takker for muligheden for at afgive høringssvar vedrørende Europa-Kommissionens forslag til forordning "Authorisation of systems providing mobile satellite services (MSS)". Vi har følgende kommentarer:

1: Der nævnes krav fra ansøgers side om, at der skal afleveres en "Annual report detailing the status of development of their proposed system". Da dette er en betingelse for at beholde licensen, og der forventes en årlig fremdrift for at beholde licensen, kunne det være relevant at kræve en revisorerklæring.

2: Derudover nævnes der under ansøgning og løbende monitorering, at f.eks. cybersecurity requirements fra gældende lovgivning og standarder skal følges og monitoreres, men det er ikke specificeret, hvorledes dette skal ske i praksis og verificeres. Der er forslag om, at monitoreringen skal foregå i medlemslandene, men en ensartet struktur f.eks. med en ISAE 3000-revisorerklæring som på f.eks. NIS 2 eller NSIS ville være nærliggende at foreslå:

> *Afsnit 26 i Proposal:*
> *Furthermore, the Union authorisation should ensure compliance with the highest applicable cybersecurity requirements, and require appropriate measures to guarantee the integrity, security and resilience of the system components and their operation, thereby safeguarding the priority and continuity of governmental communications services.*

3: Ligeledes fremhæves det, at der skal være compliance til kravene både ved ansøgning samt monitorering løbende af både regelsæt vedrørende cybersecurity, brug af netværket og f.eks. brug af data (f.eks. GDPR). Men der er ingen specifikke krav til,

hvorledes dette skal monitoreres og afrapporteres. Her kunne revisorerklæringer f.eks. på ISAE 3000-rammeværket anvendes for at lette omkostningerne og sikre en ensartet rapportering og compliance på tværs af EU:

> *Article 7 & 11:*
> *Applicants are to show satisfactory compliance with pre-requisites 1 to 4 as set out in the Annex;*
>
> *Article 9 & 10:*
> *Entrants are to;*
> *(f) with respect to cybersecurity and data security, not be subject to the jurisdiction of a third country requiring them to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited or not be subject to jurisdiction of a third country against which there is a public statement on behalf of the Union or any Member State that threat actors operating out of the territory of that third country have carried out malicious cyber activities or campaigns;*
> *(g) to be covered by one or more appropriate ITU filings related to the 2 GHz MSS band and to take all necessary measures ensuring compliance of the proposed commercial MSS system with the ITU Radio Regulations.*
>
> *Article 19:*
> *Monitoring of compliance of holders for Union authorization for use of band*

Vi står gerne til rådighed for uddybninger.

På vegne af FSR – danske revisorers Cybersikkerhedsudvalg.

Med venlig hilsen
Tina Juul
fagkonsulent