THE EU'S NEW SPACE ACT – AND THE IMPLICATIONS FOR BUSINESSES

On 25 June 2025, the European Commission unveiled its proposal for a "Space Act", which will establish a unified regulatory framework governing space operations across the European Union, with particular emphasis on cybersecurity resilience and risk management. The proposed legislation represents the EU's response to the growing importance of space infrastructure in Europe's digital economy and security architecture, introducing binding obligations that will transform how space operators approach cybersecurity and operational resilience.

24 July 2025

Focus on Comprehensive Cybersecurity Framework and Risk Management

The cornerstone of the Space Act lies in its sophisticated approach to cybersecurity governance for space infrastructure. The legislation establishes dedicated cybersecurity requirements that function as sector-specific rules, taking precedence over general EU cybersecurity frameworks where space operations are concerned. Space operators will be mandated to develop comprehensive risk management systems covering the complete operational lifecycle - including initial design phases, manufacturing processes, launch operations, in-orbit activities, and final decommissioning procedures.

The cybersecurity framework requires operators to use protective measures across their entire supply chain infrastructure. Critical security obligations include implementing stringent access controls and physical protection systems for both ground and space-based assets. Real-time cybersecurity incident detection and response capabilities are mandatory, with systems required to maintain operational continuity even during security breaches.

Communications protocols and control systems must utilise secure, certified encryption technologies - a direct response to increasing vulnerabilities in satellite command systems and mission-critical data transmission. The legislation introduces mandatory incident notification requirements, with operators required to report significant security events to senior management, governing bodies, space regulators, and NIS 2 authorities within specified timeframes ranging from 12 to 72 hours depending on incident severity.

Expanded Jurisdictional Scope and Third-Country Application

The Space Act's cybersecurity obligations extend beyond traditional EU boundaries, applying to non-EU entities that provide space services to EU operators or manage space assets serving the European market. This extraterritorial application creates regulatory obligations for third-country operators unless their legal regime has been deemed equivalent by the EU. The broad definitional scope includes entities conducting space services including spacecraft operations, launch and control facility management, and space-based data processing activities.

The legislation will reshape compliance expectations across multiple industry sectors, affecting established operators and emerging market participants alike. Satellite operators delivering broadband services, earth observation capabilities, navigation systems, and other space-based services will face binding cybersecurity obligations that exceed current fragmented national requirements. Launch service providers, component manufacturers, telecommunications companies operating satellite constellations, and space access facilities including spaceports will all fall within the regulatory framework.

The Space Act includes third-country operators and international organisations providing space-based services within EU, creating comprehensive regulatory coverage that transcends traditional jurisdictional limitations.

Enhanced Management Accountability and Compliance Obligations

A distinctive feature of the Space Act is the introduction of direct personal liability for management bodies of space operators. The governing body (including boards of directors) will bear personal responsibility for organisational compliance with the Space Act's risk management requirements. This accountability framework mirrors similar provisions in other EU cybersecurity legislation and represents a widening in executive responsibility.

The compliance framework includes comprehensive obligations, including universal hazard risk management protocols; cybersecurity risk assessment procedures; asset management and access control systems; encryption implementation; testing programmes; incident response and regulatory notification systems; and supply chain management frameworks. Space operators must establish technical policies governing encryption and backup procedures, implement IT testing programmes including threat-based penetration testing, and maintain third-party risk management systems with comprehensive asset inventories essential for space mission control.

Many cybersecurity obligations align with existing EU cybersecurity frameworks such as DORA and NIS 2, suggesting organisations may leverage existing compliance infrastructure for Space Act implementation.

Enforcement Mechanisms and Financial Penalties

Member state regulators and the EU Agency for the Space Programme (EUSPA) will possess extensive enforcement authority, including powers to conduct on-site inspections within and beyond EU territory. The enforcement framework includes substantial financial penalties, with fine levels determined by individual member states, while the Commission retains authority to impose GDPR-style penalties up to 2% of global revenue. Experience with DORA implementation suggests member states will likely authorise similar penalty levels.

In severe cases - particularly involving third-country operators - the Commission and EUSPA may intervene directly through suspension or withdrawal of authorisations and registrations, effectively restricting EU market access.

Integration with Existing Cybersecurity Frameworks

The space sector currently falls within NIS 2 scope, with NIS 2 obligations applying until the Space Act becomes effective. Upon implementation of the Space Act, it will supersede NIS 2's cybersecurity risk management obligations for space operators. This transition marks a development toward more specialised, sector-specific cybersecurity requirements recognising the unique operational challenges and security vulnerabilities of space infrastructure.

Economic Impact and Implementation Costs

The compliance requirements introduce substantial operational costs for space operators. Commission impact assessments estimate launch service providers may incur additional expenses between EUR 200,000 and 1,500,000 per mission, while satellite operators could experience 10% increases in manufacturing and operational expenditures.

Implementation Timeline and Transitional Arrangements

The current Space Act proposal establishes an implementation date of 12 January 2030, with most obligations taking effect following an eighteen-month transitional period. Space missions launched prior to 1 January 2030 are explicitly exempted from certain new requirements, providing regulatory continuity for existing planned operations.

Companies operating in the space sector should commence immediate preparations by assessing their operations' exposure to Space Act cybersecurity obligations and by evaluating their opportunities to repurpose existing cybersecurity compliance programmes.

Our Comments

The EU's proposed Space Act represents a development in space sector regulation, establishing cybersecurity obligations that will reshape space operators' approach to security and risk management. For companies with European space market exposure, understanding and preparing for these requirements is essential, regardless of their geographical establishment.

The extraterritorial application means non-EU operators serving the European market must comply with the cybersecurity requirements. The personal liability provisions for management bodies emphasise the EU's serious approach to space cybersecurity, making board-level engagement and oversight critical.

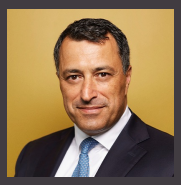
Companies should begin immediate preparations through cybersecurity posture assessments, supply chain security arrangement reviews, and incident response capability establishment. The substantial penalties and enforcement powers available to regulators make non-compliance costs potentially large and far exceeding proactive compliance measure investments.

The harmonisation of previously fragmented national approaches, while creating new compliance burdens, will ultimately provide enhanced legal certainty and a more predictable regulatory environment for space operators across the EU.

Moalem Weitemeyer continuously monitors developments in EU space and cybersecurity regulation and is available to assist with interpretation of, and compliance with, the emerging EU Space Act framework.

If you have any questions or require further information regarding any of the above, please do not hesitate to contact us.

Contacts



Dan Moalem
Partner, Chairman
dan.moalem@moalemweitemeyer.com

Thomas Mygind
Partner
thomas.mygind@moalemweitemeyer.com

Andjela Parezanovic
Associate
andjela.parezanovic@moalemweitemeyer.com

If you have any questions or require further information regarding any of the above, please do not hesitate to contact us.