Key Considerations for Global Investors in the Defence Sector

Moalem Weitemeyer

Introduction

Global investors continue to show strong appetite for the Danish defence sector, supported by a rapidly expanding European investment landscape.

Majority investments by Bridgepoint in MyDefence and UMag Solutions, Fjord Defence Group's acquisition of Scanfiber Composites as well as a series of foreign-backed funding rounds involving Danish defence technology companies demonstrate international investors seeking exposure to the sector. On the funding side, the Security Action for Europe ("SAFE") instrument provides up to EUR 150 billion in EU-backed loans for defence procurement(1). More broadly, the ReArm Europe Plan/Readiness 2030 aims to unlock up to EUR 800 billion in additional defence investment, while the European Commission's Defence Readiness Omnibus seeks to facilitate that investment by simplifying the regulatory framework applicable to the defence industry(2).

In this newsletter, partners Dan Moalem, Pernille Nørkær and Thomas Enevoldsen and Associate Sumar Adely break down some of the key considerations for global investors in the Danish defence sector from a legal/regulatory perspective. Beyond the core approval regimes and recent legislative updates, we also cover key diligence areas from a process and substance perspective, including security clearances for the workforce and the practical limits of due diligence in a security-sensitive business.

1) Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument
2) European Commission, ReArm Europe Plan/Readiness 2030, SAFE.

Regulatory Framework

Three separate regimes may apply when it comes to foreign investments in the Danish defence sector.

1. The Danish Investment Screening Act, Denmark's general FDI regime, require mandatory pre-closing screening of foreign investments (from 10% ownership or voting interest) in sensitive sectors such as defence and certain dual-use activities. The statutory deadline for a phase 1 (simple) approval is 45 calendar days. Deadline for phase 2 can be up to 125 calendar days.

2. The Danish War Materials Act governs manufacturing and storage licences for war material. The scope follows the EU Common Military List(3) and covers weapons and ammunitions as well as a broad range of other military products such as vehicles and drones, protective equipment as well as certain software with military applications. The act requires approval of foreign ownership (above 20%), control and financing. There is no statutory deadline for processing approvals, however our experience indicates 6–8 weeks for initial assessment.

3. Conditions of export licences can be affected by change in ownership. Export control determines on what conditions sensitive products, software or technology may be exported out of Denmark and may cover both physical and electronic products. While there is no regulatory approval regime for ownership changes, export licenses can be conditional upon ownership and control structures. Expansion plans may also be affected by what end user permissions and transfers.

3) C/2026/1640 Common Military List of the European Union as adopted by the Council on 23 February 2026 regarding equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment (updating and replacing the Common Military List of the European Union adopted by the Council on 24 February 2025).

Decisions under FDI and the Danish War Materials Act are confidential and not published as precedents. Predictability is based on the statutory scope of each regime, authority guidance and process experience.

Updates to the Dual-Use Regulation

The European Commission has adopted an updated Annex I to Regulation (EU) 2021/821 on the control of exports, brokering, technical assistance, transit and transfer of dual-use items (the "Dual-Use Regulation"), introducing and revising controls on strategically sensitive technologies, including semiconductor manufacturing and testing equipment, advanced computing integrated circuits, additive manufacturing equipment and gas-turbine technology. The updated list is expected to enter into force in mid-November 2026 (following the applicable scrutiny period)(4).

In parallel, the Commission has commenced an overall evaluation of the Dual-Use Regulation, including its rules on cyber-surveillance items. The consultation remains open and may lead to further changes to the export control framework. Investors should continue to monitor product classifications and licensing requirements, particularly for businesses exposed to emerging technologies(5).

4) European Commission, "2026 Update of the EU Control List of Dual-Use Items", 14 September 2026.
(5) European Commission, "Open Public Consultation and Call for Evidence – Overall Evaluation of Regulation (EU) 2021/821", opened 23 July 2026, deadline 15 October 2026.

From an investment perspective, the consequence of the new Dual-Use Regulation may be that a Danish technology or industrial company that was not previously treated as a producer of dual-use products can now become subject to mandatory FDI screening.

Sponsors looking at signing/closing of investments in Q4 2026 should design their processes around an expected expanded FDI scope when the updated Dual-Use Regulation enters into force.

Due Diligence

Many defence-sector targets have dual-use product/service portfolios and thus sell to the civilian sector as well. By nature, the transaction process for those targets will largely follow a conventional M&A playbook, including in respect of due diligence.

The following areas typically require particular attention when it comes to investments in the defence-sector:

i. **Real estate**: facilities used for defence-related activities are typically subject to physical-security requirements, including surveillance, access control and secure storage.

ii. **Contracts**: Where direct review of classified contracts is restricted, a structured Q&A process can address key issues, including change-of-control provisions, termination rights, minimum purchase commitments, notice periods, cleared-personnel requirements and restrictions on subcontracting.

iii. **IP and technology**: defence-related intellectual property may be subject to contractual limitations on ownership, licensing or transfer under government contracts, conditions attached to public funding, and export-control requirements.

iv. **Cybersecurity**: Targets providing digital, communications or infrastructure services should be assessed for NIS2-compliance, including supply-chain risk measures, incident-response and reporting procedures. NIS 2 implementation remains relatively immature across parts of the Danish corporate sector as applicability is based on self-assessment and obligations are risk-based rather than prescriptive.

v. **Industrial Cooperation**: Dependencies on foreign defence primes from industrial cooperation arrangements (in Danish: *industrisamarbejde*) from Danish defence procurement should be assessed. Any planned post-closing restructuring or relocation should could jeopardize qualification as a Danish industrial-cooperation partner.

Security Clearances

For core defence-sector targets, security clearances may form part of both the due diligence process as well as within the target itself, both on an entity and employee-level.

In Denmark, employees with access to classified information require an individual security clearance. A clearance for TOP SECRET information is valid for up to five (5) years, while clearances for SECRET or CONFIDENTIAL information can remain valid for up to ten (10) years. Foreign individuals can in principle obtain a Danish security clearance, but foreign nationality is itself a relevant factor in the background review, and this should be tested early for any non-Danish personnel expected to work on sensitive contracts.

From a transaction perspective, the Danish Defence Intelligence Service (in Danish: *Forsvarets Efterretningstjeneste*) must be informed as soon as a change of ownership or merger is contemplated for a target holding a company security clearance. Investors should therefore assess early whether board composition and governance arrangements could affect the target's approval or restrict access to classified information, particularly where foreign owners or directors are involved.

From an operational perspective, due diligence should review applicable day-to-day measures such as access controls, secure facilities and information-security management system and how that fits into integration plans for the target. Companies holding security clearances are expected to assess security risks continuously and report incidents immediately. Appropriate transaction protections should therefore include regulatory cooperation covenants, conditions relating to continued security approval and specific remediation commitments as needed.

Key Takeaways

The central question for investors is two-fold: does the target comply with defence-sector regulation today, and can it continue to operate as intended under future owner-ship and growth plans. Changing ownership may trigger both regulatory transaction approval process as well as operational clearances and permits, including in respect of access to classified information, use of foreign directors and employees, and ability to share technology or data with other group companies. These issues can influence the transaction structure, timetable and post-closing integration plan.

Regulatory planning should be an early transaction consideration to map the target’s activities, products, licences, clearances and key contracts against the investor’s owner-ship structure and intended operating model. Some issues may be managed through engagement with authorities, governance arrangements and covenants in the transaction documents. If identified late, however, they may delay closing, require changes to the proposed structure or limit the investor’s ability to integrate the target.

Contacts

Dan Moalem

Chairman, Partner

dan.moalem@moalemweitemeyer.com

Pernille Nørkær

Partner, Head of Disputes & Investigations

pernille.noerkaer@moalemweitemeyer.com

Thomas Enevoldsen

Partner

thomas.enevoldsen@moalemweitemeyer.com

Sumar Adely

Associate

sumar.adely@moalemweitemeyer.com