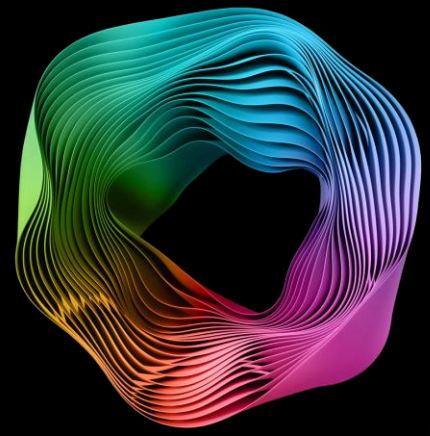




Classified Information Protection

Classified Information Protection refers to the measures and regulations that companies must implement and comply with in connection with classified government contracts ("VS-Aufträge") to protect confidential state information. In light of the growing cooperation between government and industry, the topic has become a strategic priority in day-to-day business operations. The ability to handle classified information securely is no longer a challenge limited to established companies in the security and defense sector. Rather, as new forms of cooperation and increasingly complex supply chains emerge in connection with public procurement, industrial security is becoming increasingly relevant for companies of various sizes and across a wide range of industries.

Legal framework

The purpose of Classified Information Protection is to protect information that has been classified as official secrets. The applicable requirements are derived primarily from the German Security Clearance Act (Sicherheitsüberprüfungsgesetz – SÜG), the relevant Classified Information Directive (Verschlusssachenanweisung – VSA), and other security regulations, including in particular the Classified Information Protection Handbook (Geheimsschutzhandbuch – GHB) issued by the Federal Ministry for Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie – BMWI).

Classified Information Protection is divided into two fundamental areas: personnel security and physical security. Personnel security concerns individuals who, as part of their professional duties, handle classified information. It focuses on ensuring that such individuals meet the necessary security requirements and can be entrusted with access to classified material. Physical security relates to the protection of classified information and assets against unauthorized access. This includes, in particular, secure access controls, the safeguarding of facilities and storage locations, and the implementation of appropriate information security and IT security measures.

Legal, operational and strategic challenges

The issue of classified information protection poses specific, often completely new challenges for companies. There is a complex tension between confidentiality requirements on the one hand and general regulatory requirements on the other. In addition, increased security measures affect operational processes. This creates tension between security requirements and other strategic goals such as efficiency, flexibility, and speed of innovation.

The topic must therefore be considered holistically in conjunction with existing legal requirements, operational processes, and business strategies. Areas of conflict must be identified and made legally compliant and practicable. At the same time, overlaps with existing regulatory requirements (e.g., in the area of IT security) should be identified in order to exploit potential synergies.



Why act now? The number of potentially affected companies is rising. Companies that make their organization “public ready” position themselves as reliable partners in an increasingly security-conscious environment and secure competitive advantages.

ACTION FIELDS

Tasks

Companies operating in the public sector should address the issue of Classified Information Protection at an early stage so that they can respond quickly to any requirements that may arise.

Preparation for and compliance with Classified Information Protection requirements typically involve, in particular, the following tasks:

- ✓ **Impact assessment:** Evaluation of existing and (strategically) anticipated contracts and supply chains, identification of potential areas for action
- ✓ **Public Ready Assessment:** Assessment of the current status quo with regard to technical and organizational measures, in particular IT security, internal processes, personnel deployment, governance structures, and contracts; identification of areas for action and necessary measures
- ✓ **Strategic alignment:** Preparatory measures with regard to planned market entry or expansion, in particular preparation of Classified Information Protection supervision, positioning in supply chains, development of personnel and training
- ✓ **Legal Risk Assessment:** Identification of potential conflicts with other legal obligations, particularly in the areas of corporate law, labor law, contract law and export control
- ✓ **Synergy Assessment:** Identification of potential synergies in connection with existing or planned technical and organizational measures and processes (e.g., in the areas of IT security, human resources management, vendor management)
- ✓ **Design and implementation of measures for Classified Information Protection:** Measures relating to personnel security and physical security measures – including the adjustment or establishment of corporate and governance structures, the revision of existing contracts, the drafting of new contracts, and the adjustment or implementation of export control systems

Our Offering

Deloitte Legal & Deloitte: As One Deloitte we provide you with comprehensive support

- ✓ **Comprehensive assessment and support with regard to legal, technical and organizational requirements**
- ✓ **Development of legally and operationally relevant frameworks, e.g., internal regulations and guidelines, governance, processes**
- ✓ **Review and structuring of legal relationships and matters**

YOUR CONTACT

We provide comprehensive advice on classified information protection requirements, their implementation, and all related legal issues. For interdisciplinary advice, we combine our legal expertise in proven collaboration with other experts from Deloitte to jointly provide the necessary comprehensive and interdisciplinary support in this field.



Dr. Söntje Julia Hilberg, LL.M.

Lawyer | Partner
Co-Lead Digital Law
E-Mail: shilberg@deloitte.de
Phone: +49 30 254683016
Mobile: +49 170 7663353



Dennis Buschmann, LL.M. B.A.

Lawyer | Senior Manager
E-Mail: dbuschmann@deloitte.de
Phone: +49 30 254681886