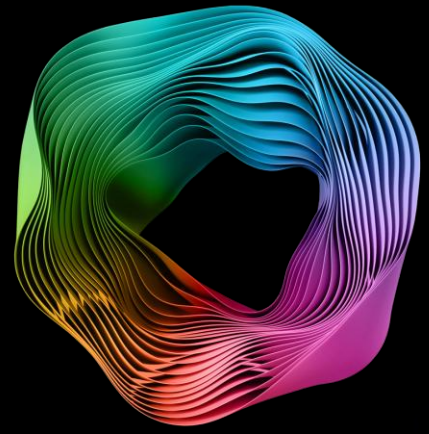




Geheimschutz in der Wirtschaft

Geheimschutz in der Wirtschaft bezieht sich auf Maßnahmen und Vorschriften, die Unternehmen im Zusammenhang mit sog. VS-Aufträgen ergreifen bzw. einhalten müssen, um vertrauliche staatliche Informationen zu schützen. Das Thema wird mit Blick auf die zunehmende Zusammenarbeit zwischen Staat und Wirtschaft zur strategischen Aufgabe im Unternehmensalltag. Die Fähigkeit zum sicheren Umgang mit Verschlusssachen ist längst nicht mehr nur Herausforderung für etablierte Unternehmen der Sicherheits- und Verteidigungsindustrie. Vielmehr betrifft das Thema Geheimchutz mit Blick auf neuartige Kooperationen und Lieferketten im Zusammenhang mit öffentlichen Aufträgen zunehmend auch Unternehmen verschiedener anderer Branchen und Größen.

Rechtsrahmen und Handlungsfelder

Ziel des Geheimschutzes ist der Schutz von als Verschlusssachen eingestuft Informationen. Die geheimchutzrechtlichen Vorgaben ergeben sich dabei unmittelbar aus den Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG), der jeweils einschlägigen Verschlusssachenanweisung (VSA) sowie den weiteren Geheimchutzvorschriften, wozu insbesondere auch das sog. Geheimchutzhandbuch (GHB) des Bundesministeriums für Wirtschaft und Energie (BMWE) zählt.

Der Geheimchutz gliedert sich in zwei elementare Bereiche: Den personellen und den materiellen Geheimchutz. Der personelle Geheimchutz betrifft die Personen, die aufgrund ihrer Tätigkeit mit Verschlusssachen umgehen. Der materielle Geheimchutz betrifft den physischen Schutz, darunter insbesondere den sicheren Zugang, von Verschlusssachen, insbesondere den Bereich der IT-Sicherheit.

Rechtliche, operative und strategische Herausforderung

Das Thema Geheimchutz bedeutet für Unternehmen spezielle, rechtliche und technisch komplexe neue Anforderungen. Nicht selten entsteht ein Spannungsfeld zwischen Anforderungen des Geheimschutzes auf der einen und allgemeinen regulatorischen Anforderungen auf der anderen Seite. Zudem können Geheimchutzmaßnahmen etablierte Betriebsabläufe und gewohnten Prozesse erheblich beeinflussen. So entstehen Spannungen zwischen Sicherheitsvorgaben und anderen Unternehmenszielen wie Effizienz, Flexibilität oder Innovationsgeschwindigkeit.

Das Thema Geheimchutz muss deshalb ganzheitlich in Verbindung mit bestehenden rechtlichen Anforderungen, operativen Prozessen sowie Unternehmensstrategien betrachtet werden. Spannungsfelder müssen erkannt und rechtssicher sowie praktikabel gestaltet werden. Gleichzeitig sollten Überschneidungen im Hinblick auf bestehende regulatorische Anforderungen (z.B. im Bereich IT-Sicherheit oder Exportkontrolle) identifiziert werden, um mögliche Synergien zu nutzen.



Warum jetzt agieren? Die Zahl der potentiell betroffenen Unternehmen steigt. Unternehmen, die ihre Organisation »public ready« gestalten, positionieren sich als verlässliche Partner in einem zunehmend sicherheitsbewussten Umfeld und sichern sich Wettbewerbsvorteile.

Aufgaben

Unternehmen, die sich im Bereich öffentlicher Aufträge bewegen, sollten sich frühzeitig mit dem Thema Geheimschutz auseinandersetzen, um auf eventuelle Anforderungen belastbar vorbereitet zu sein.

Die Vorbereitung sowie Compliance im Bereich Geheimschutz beinhaltet insbesondere folgende Aufgaben:

- ✓ **Betroffenheitsprüfung:** Prüfung bestehender und (strategisch) geplanter Aufträge und Lieferketten, Identifizierung möglicher Handlungsfelder
- ✓ **Public Ready Assessment:** Prüfung des Status Quo im Hinblick auf technische und organisatorische Maßnahmen, insbesondere IT-Sicherheit, interne Prozesse, Personaleinsatz und –entwicklung, Governance Strukturen und Verträge; Identifizierung von Handlungsfeldern und notwendigen Maßnahmen
- ✓ **Strategische Ausrichtung:** Vorbereitende Maßnahmen im Hinblick auf geplanten Markteintritt oder –ausbau, insbesondere Vorbereitung der Geheimschutzbetreuung, Positionierung in Lieferketten, Personalentwicklung und –schulung
- ✓ **Legal Risk Assessment:** Identifizierung von potentiellen Konflikten mit anderen rechtlichen Anforderungen oder Verpflichtungen, insbesondere im Zusammenhang mit Implikationen aus dem Gesellschafts-, Arbeits- und Vertragsrecht sowie der Exportkontrolle.
- ✓ **Synergie Assessment:** Identifizierung von potentiellen Synergien im Hinblick auf bestehende oder geplante technische und organisatorische Maßnahmen und Prozesse (z.B. IT-Sicherheit, Personalmanagement, Vendor Management)
- ✓ **Konzept und Implementierung von Maßnahmen zum Geheimschutz: von Maßnahmen des personellen und materiellen Geheimschutzes – einschließlich der Anpassung** oder dem Aufbau gesellschaftsrechtlicher und Governance-Strukturen sowie der Überarbeitung bestehender und Gestaltung neuer Verträge sowie Anpassung oder Gestaltung von Exportkontrollsystemen.

Unsere Services

Deloitte Legal & Deloitte: As One Deloitte beraten wir umfassend zum Thema Geheimschutz

- ✓ **Ganzheitliche Prüfung des Unternehmens im Hinblick auf die Anforderungen zum Geheimschutz**
- ✓ **Entwicklung und Begleitung der Geheimschutzorganisation, insbesondere Schaffung rechtlich und operativ relevanter Rahmenbedingungen (z.B. interne Regelwerke, Governance und Prozesse)**
- ✓ **Prüfung und Gestaltung rechtlicher Beziehungen und Sachverhalte**

IHR KONTAKT

Wir beraten Sie umfassend im Zusammenhang mit geheimschutzrechtlichen Anforderungen, deren Umsetzung und sämtlichen damit verbundenen rechtlichen Fragestellungen. Zur interdisziplinären Beratung verbinden wir unsere rechtliche Expertise in erprobter Zusammenarbeit mit weiteren Fachexperten von Deloitte, um gemeinsam die erforderliche ganzheitliche und interdisziplinäre Beratung im Bereich Geheimschutz zu liefern.



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