Geheimschutz und Sicherheitsüberprüfungen in der Privatwirtschaft

Compliance-Anforderungen in einer veränderten Sicherheitslage

5. Mai 2026

Viele Unternehmen sehen sich zunehmend mit **Anforderungen des Geheimschutzes** konfrontiert – etwa als Bieter bei öffentlichen Aufträgen im Verteidigungs- und Sicherheitsbereich oder als Zulieferer für Kritische Infrastrukturen. Die **veränderte Sicherheitslage in Deutschland und Europa** führt zu neuen **Compliance-Pflichten für die Privatwirtschaft**. Dieses Briefing richtet sich sowohl an Unternehmen, die erstmals mit geheimhaltungsbedürftigen Informationen arbeiten, als auch an Unternehmen, die schon heute über entsprechende Erfahrungen verfügen.

Zu unterscheiden ist zwischen dem **Schutz vor Industrie- und Wirtschaftsspionage** und dem **Schutz von Informationen, die im öffentlichen Interesse geheimhaltungsbedürftig** sind. Für letzteren hat der Gesetzgeber umfassende Regelungen zum **materiellen** und **personellen Geheimschutz** geschaffen, die auch private Unternehmen erfassen können.

Der personelle Geheimschutz ist im Sicherheitsüberprüfungsgesetz (SÜG) geregelt, das zuletzt im Jahr 2026 **vor dem Hintergrund neuer Gefährdungslagen** geändert wurde. Mit dem SÜG soll erreicht werden, dass nur **zuverlässige Personen** Zugang zu **sicherheitsempfindlichen Informationen** erhalten.

Kerninstrument des SÜG ist die **Sicherheitsüberprüfung (SÜ)**. Sie wird durch die zuständigen Stellen unter Mitwirkung des Bundesamts für Verfassungsschutz durchgeführt. Geprüft wird vor allem die **Zuverlässigkeit der betroffenen Person**, aber auch eine **mögliche Erpressbarkeit** sowie das **Bekenntnis zur freiheitlichen demokratischen Grundordnung**. Zentrale Grundlage der Prüfung ist die **Sicherheitserklärung**, mit der Betroffene **weitreichende Angaben** machen müssen – etwa zu Staatsangehörigkeiten, finanziellen Verhältnissen, Auslandsbezügen, sozialen Netzwerken sowie zu Ehepartnern und nahen Angehörigen in sicherheitsrelevanten Staaten.

Geheimhaltungsbedürftige Informationen werden als **Verschlusssachen (VS)** eingestuft. Das SÜG unterscheidet **vier Geheimhaltungsgrade**, die jeweils unterschiedliche Anforderungen auslösen:

- VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD): Keine SÜ, aber organisatorische Mindestmaßnahmen und förmliche Verpflichtung der Beschäftigten
- VS-VERTRAULICH: Einfache Sicherheitsüberprüfung (Ü1)

- **GEHEIM**: Erweiterte Sicherheitsüberprüfung (Ü2)
- **STRENG GEHEIM**: Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3)

Flankiert wird der Geheimschutz durch **strafrechtliche Vorschriften zum Schutz von Staatsgeheimnissen**. Das Geheimschutzhandbuch (GHB) des Bundesministeriums für Wirtschaft und Energie konkretisiert die **organisatorischen und technischen Anforderungen** an Unternehmen mit VS-Zugang.

Was haben Unternehmen zu beachten, die erstmals mit eingestuften Dokumenten arbeiten?

- Unternehmen, die erstmals mit geheimhaltungsbedürftigen Unterlagen arbeiten, müssen sich frühzeitig auf **umfangreiche regulatorische Anforderungen** einstellen. Bereits für einen Umgang mit Unterlagen, die als VS-NfD eingestuft sind, sind **grundlegende organisatorische Maßnahmen** erforderlich, insbesondere klare **Zuständigkeiten**, **Dokumentationspflichten** und die **förmliche Verpflichtung der Beschäftigten**. Schon als VS-NfD eingestufte Dokumente sind **physisch in einer Weise aufzubewahren**, mit der eine **Kenntnisnahme durch Unbefugte ausgeschlossen** wird. Bei der IT-Infrastruktur ist auf eine **angemessene Firewall**, den **Schutz vor Schadprogrammen** und eine **verschlüsselte Übertragung** zu achten.

- Ab einem höheren Geheimhaltungsgrad sind **Sicherheitsüberprüfungen zwingend** durchzuführen. Dazu ist ein Geheimschutzvertrag mit dem BMWE abzuschließen, der das betroffene Unternehmen der **Geheimschutzbetreuung des Bundes** unterstellt und mit dem das betroffene Unternehmen die **Vorgaben des GHB als verbindlich** anerkennt. In der Praxis bedeutet dies häufig einen erheblichen Anpassungsbedarf in den Bereichen **IT-Sicherheit, Personalorganisation und physische Sicherheit**. Betroffene Unternehmen müssen beispielsweise als **zentrales Sicherheitsorgan im Unternehmen** einen **Sicherheitsbevollmächtigten** sowie – bei bestimmten Tätigkeiten – einen **Sabotageschutzbeauftragten** benennen. Diese Funktionen müssen **von der Personalverwaltung getrennt** sein und sind regelmäßig mit **Schulungs- und Sensibilisierungsaufgaben** betraut. Es empfiehlt sich, mit diesen Aufgaben **Personen in leitender Funktion** zu betrauen.

- Unternehmen mit **Auslandsbezug oder Tätigkeiten im NATO- oder EU-Kontext** müssen darüber hinaus **ausländische und internationale Geheimschutzstandards** berücksichtigen. Hinzu kommen neue **sektorübergreifende Anforderungen**, etwa aus der NIS-2-Richtlinie und dem KRITIS-Dachgesetz, die insbesondere im Bereich der Cybersicherheit Überschneidungen mit dem Geheimschutz

nach dem SÜG aufweisen. **Compliance-Konzepte** sollten sich nicht allein auf eines dieser Regelwerke beziehen.

- Die betroffenen Personen müssen sich auf eine gewisse **Dauer der Sicherheitsüberprüfung** einstellen, die – je nach Art der SÜ – **mehrere Wochen oder Monate** in Anspruch nehmen kann. Unvollständige oder fehlerhafte Sicherheitserklärungen führen **regelmäßig zu Verzögerungen**. Zudem sind Zuständigkeitsfragen zu klären, da neben dem SÜG des Bundes auch **16 landesrechtliche Regelungen** existieren.

Was haben Unternehmen zu beachten, die heute schon mit geheimhaltungsbedürftigen Informationen arbeiten?

- Unternehmen mit laufendem VS-Zugang müssen den **Geheimhaltungsgrad** der eingestuften Unterlagen überwachen. Sobald die **Schwelle von VS-NfD zu VS-VERTRAULICH** überschritten wird, ist die **Geheimschutzbetreuung zwingend**.

- Gegenüber **Lieferanten und Nachunternehmern** sind Unternehmen mit laufendem VS-Zugang verpflichtet, auf die **Einhaltung der entsprechenden Standards** zu achten. Die Regelungen zum Schutz von VS-NfD-Dokumenten bzw. das GHB müssen zum **Vertragsbestandteil** mit anderen Unternehmen gemacht werden. Auch ein **nicht-öffentlicher Auftraggeber** muss gegenüber seinen Auftragnehmern **die Einhaltung von Geheimhaltungsstandards** kontrollieren.

- Unternehmen in Geheimschutzbetreuung sind verpflichtet, **Wiederholungsüberprüfungen fristgerecht** durchzuführen und sicherzustellen, dass **sicherheitserhebliche Veränderungen in der Person des Beschäftigten** – etwa neue familiäre Bindungen, Straf- oder Insolvenzverfahren – **unverzüglich gemeldet** werden.

- Angesichts der aktuellen Sicherheitslage gewinnt zudem der **personelle Sabotageschutz** an Bedeutung, der teilweise eigenständigen Regelungen im SÜG folgt. Parallel rücken der **Schutz der physischen Unternehmensinfrastruktur** sowie die **Resilienz gegen hybride Bedrohungen** stärker in den Fokus. Für betroffene Unternehmen ist Geheimschutz daher nicht nur eine formale Pflicht, sondern ein **dauerhaftes Governance- und Risikomanagement-Thema.**

***

BLOMSTEIN wird Sie über die weiteren Entwicklungen auf dem Laufenden halten. Bei Beratungsbedarf und anderen Fragen zu Geheimschutz und Sicherheitsüberprüfungen in der Privatwirtschaft stehen Ihnen Dr. Christopher Wolters, Dr. Laura Louca, Konstantin Kuhle, Hanna Sophie Vetter sowie das gesamte Team jederzeit gerne zur Verfügung.

BLOMSTEIN | Wir beraten unsere internationalen Mandanten in den Gebieten Kartell-, Vergabe-, Außenwirtschafts- und Beihilferecht sowie ESG in Deutschland, Europa und – über unser globales Netzwerk – weltweit.