

# NEUE CYBER-SECURITY-REGELN IN DEUTSCHLAND—REGISTRIERUNGSPFLICHT LÄUFT AM 6. MÄRZ 2026 AB

Date: 5 März 2026

## EU Corporate and Policy and Regulatory Alert

By: Dr. Thomas Nietsch, Dr. Ulrike Elteste

Mit einer Verspätung von mehr als einem Jahr ist im Dezember 2025 das deutsche Umsetzungsgesetz zur [NIS2-Richtlinie](#) (Richtlinie (EU) 2022/2555 in Kraft getreten ([Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung](#))). Das Gesetz sieht erhebliche Änderungen und Neugestaltungen verschiedener Cyber-Security-Gesetze vor, insbesondere des [BSI-Gesetzes](#).

Sehr viel mehr Unternehmen als zuvor fallen nun in den Anwendungsbereich des BSI-Gesetzes. Zuvor wurden im BSI-Gesetz nur klassische kritische Infrastruktur wie Transport und Verkehr, Energie, Finanzwesen, Gesundheit, Forschung und die Telekommunikationsindustrie reguliert. Jetzt ist auch der Digitalsektor erfasst, insbesondere Cloud Computing-Dienste, Rechenzentrumsbetreiber, Managed (Security) Services Provider sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und sozialen Netzwerken. Auch Produktion und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln sowie verschiedene Bereiche des verarbeitenden Gewerbs (Produktion von Waren) sind betroffen. Listen der erfassten Sektoren und Tätigkeiten sind [hier](#) und [hier](#) abrufbar. Das BSI bietet auf seiner Website eine [Betroffenheitsprüfung](#) an.

Obwohl von der Richtlinie so nicht vorgesehen, sieht das deutsche Umsetzungsgesetz eine *de minimis*-Ausnahme vor, wenn eine grundsätzlich erfasste Tätigkeit im Hinblick auf die Gesamttätigkeit eines Unternehmens vernachlässigbar sind. In diesen Fällen gelten die Anforderungen des BSI-Gesetzes nicht.

Erfasste Einrichtungen müssen sich bis zum 6. März 2026 auf der vom BSI bereitgestellten [Plattform](#) registrieren. Dies erfordert ein ELSTER-Organisationszertifikat.

Bei Verstoß droht ein Bußgeld von bis zu EUR€500.000. Aber auch unabhängig davon sollten Unternehmen gründlich prüfen, ob sie in den Anwendungsbereich des Gesetzes fallen und welche Pflichten das für sie mitbringt.

Weitere Pflichten von erfassten Unternehmen umfassen insbesondere:

- Ergreifen von angemessenen Maßnahmen zur Vermeidung und Behebung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme;
- Unverzögliche Meldung von erheblichen Sicherheitsvorfällen an eine einheitliche Meldestelle;
- Schulungspflichten

Für Verstöße gegen diese Pflichten ist die Geschäftsführung ihrem Unternehmen gegenüber auf Schadensersatz haftbar.

## KEY CONTACTS



**DR. THOMAS NIETSCH**  
PARTNER

BERLIN  
+49.30.220.029.408  
THOMAS.NIETSCH@KLGATES.COM



**DR. ULRIKE ELTESTE**  
COUNSEL

FRANKFURT  
+49.69.945.196.416  
ULRIKE.ELTESTE@KLGATES.COM

---

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.