Aulinger

Südwestfalen Protected · 23.09.2025

(Persönliche) Haftung im Zeitalter von NIS-2 und BSIG-E: Was Führungskräfte jetzt wissen müssen

Dr. Ralf Heine M.M.

Rechtsanwalt · Fachanwalt für Arbeits- und IT-Recht

Dr. Ralf Heine M.M.

Rechtsanwalt | Partner

Tel. +49 201 9598648

ralf.heine@aulinger.eu

Qualifikation

- mehr als 15 Jahre Berufserfahrung in den Bereichen Arbeitsrecht, IT- und Datenschutzrecht
- Fachanwalt für Arbeitsrecht und Informationstechnologierecht
- zert. Datenschutzauditor- und beauftragter
- gelistet als einer der „**Best Lawyers Germany – IT-Recht**“ 2024

Tätigkeitsschwerpunkte

- Rechtssichere und risikominimierende Gestaltung von IT-Verträgen sowie Nutzungsbedingungen
- Geltendmachung von und Verteidigung gegen Schadensersatzansprüche im IT-Bereich
- Verhandlungen von Datenschutzverträgen
- Erstellung der erforderlichen Datenschutzdokumentationen
- Führen von Auseinandersetzung mit Datenschutz-Aufsichtsbehörden in einem datenschutzrechtlichen Kontroll- oder Bußgeldverfahren

Aulinger

Agenda

1. Einführung und Zielsetzung
2. Rechtliche Grundlagen der Compliance
3. Compliance-Risiken und praktische Fallstricke
4. Technische und organisatorische Maßnahmen
5. Barrierefreiheit und Compliance
6. Drittlandtransfer und internationale Compliance
7. Praktische Umsetzung und Tipps für den Arbeitsalltag
8. Fazit

1. Einführung

Einführung

Die NIS2-Richtlinie - worum geht es?

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Die NIS2-Richtlinie - worum geht es?

- rechtliche Maßnahmen zur **Steigerung des Gesamtniveaus der Cybersicherheit** in der EU
- **Erschaffung und Verbesserung** eines **einheitlichen Sicherheitsniveau** in den Mitgliedstaaten der EU
- Grundsatz der **Mindestharmonisierung**

- **Umsetzung** der NIS2-Richtlinie in nationales Recht durch **Änderung des BSI-Gesetzes**

- nach Schätzungen fallen ca. **30.000 Unternehmen** deutschlandweit (unmittelbar) in den Anwendungsbereich der NIS2-Richtlinie
- Unternehmen müssen **angemessene, wirksame und geeignete Risikomanagementmaßnahmen** umsetzen, dokumentieren und regelmäßig überprüfen lassen

2. Aktueller Stand der Umsetzung

Aktueller Stand der Umsetzung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Aktueller Stand der Umsetzung

Aufgrund der vorgezogenen Wahlen konnte das parlamentarische Verfahren zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) nicht abgeschlossen werden. Die Umsetzung der NIS-2 Richtlinie bleibt weiterhin vordringlich.

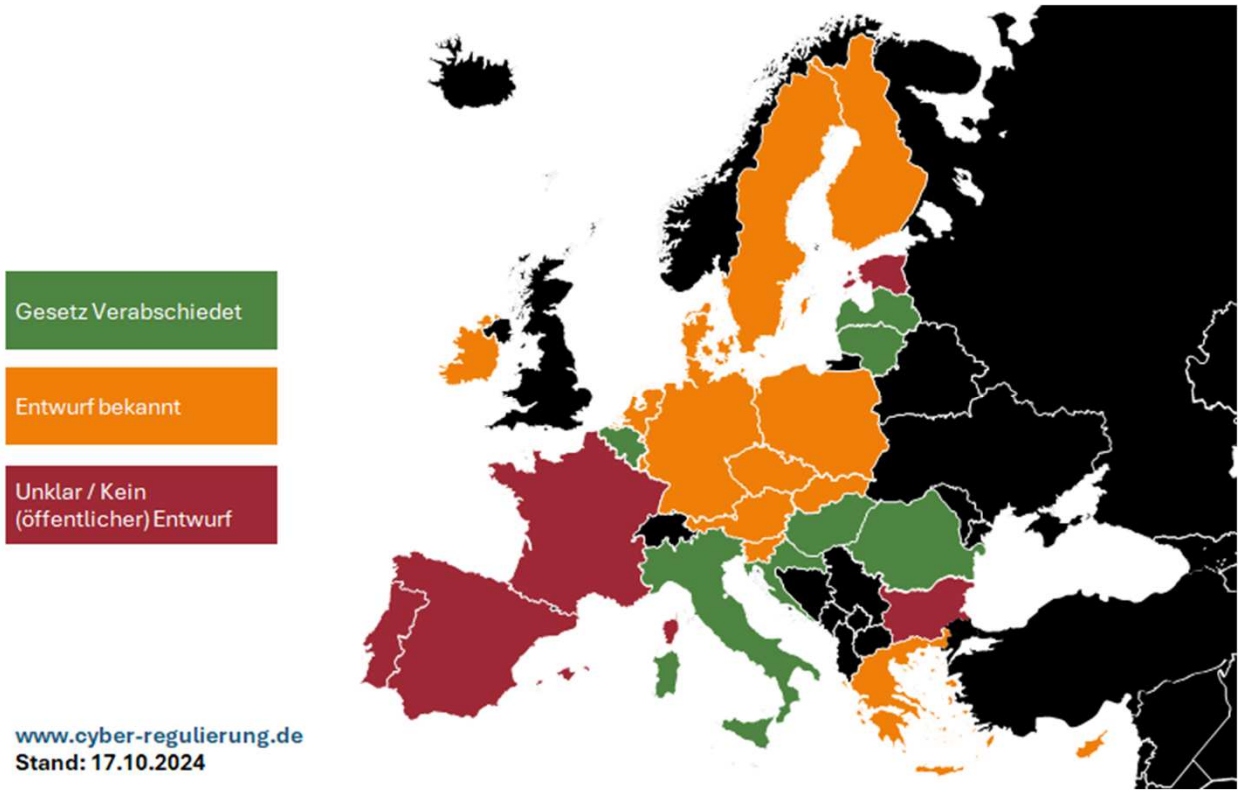
Quelle: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html (Abruf vom 08.04.2025)

Aktueller Stand der Umsetzung

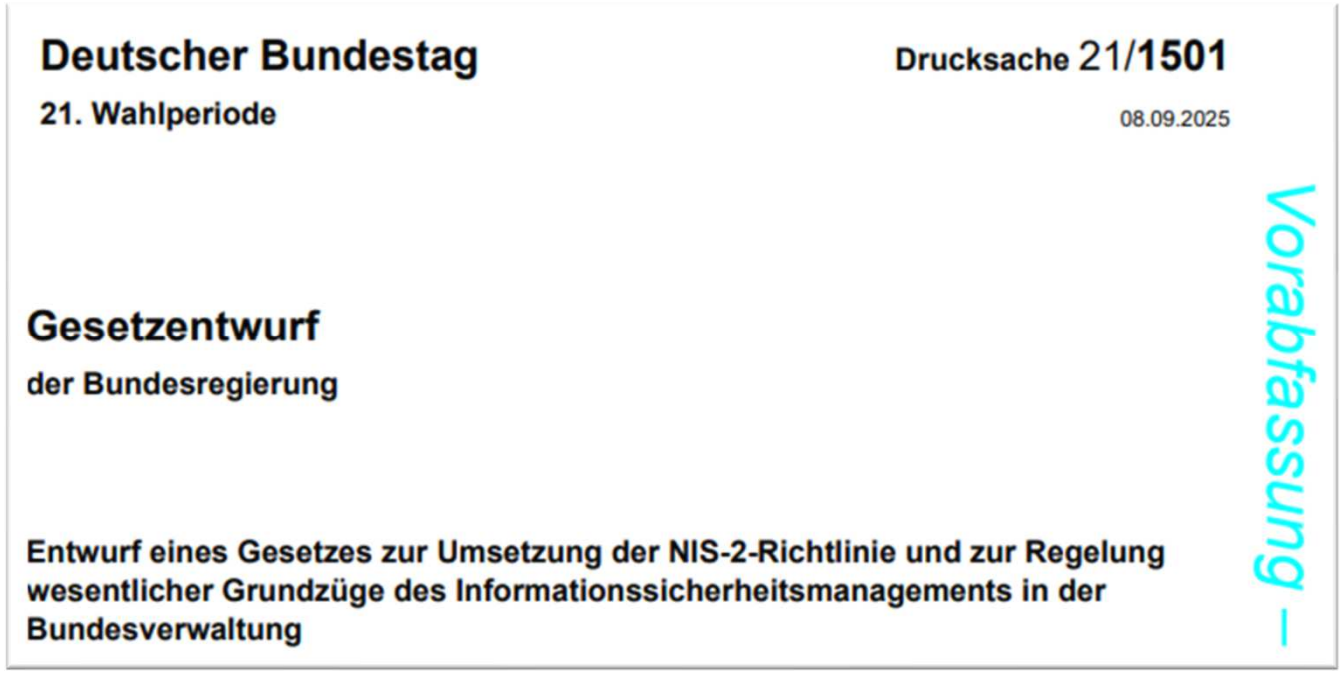
- NIS2UmsuCG konnte wegen der **vorgezogenen Bundestagswahl** nicht mehr verabschiedet werden
- **Diskontinuitätsprinzip** für nicht-verabschiedete Vorlagen greift

- EU hat **Vertragsverletzungsverfahren** gegen Deutschland und weitere 22 EU-Mitgliedsstaaten eingeleitet

Aktueller Stand der Umsetzung



Aktueller Stand der Umsetzung



Deutscher Bundestag

21. Wahlperiode

Drucksache 21/1501

08.09.2025

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

– Vorabfassung –

(mögliche) Unmittelbare Wirkung

Eine Richtlinie hat **unmittelbare Wirkung**, wenn:

- ihre Bestimmungen **uneingeschränkt und hinreichend klar und eindeutig** sind und
- wenn der Mitgliedstaat die Richtlinie **nicht fristgerecht umgesetzt** hat

- Aufsichtsmaßnahmen greifen nicht, da Behörden für Eingriffe Rechtsgrundlage brauchen
- Sorgfaltspflichten und Haftungsregelungen für Einrichtungen können u.U. im privatrechtlichen Rechtsverkehr nicht ausgeschlossen werden

3. Was gilt bereits jetzt?

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

- Cybersicherheit nicht nur für Kritische Infrastrukturen, sondern **flächendeckend als allgemeine Compliance-Anforderung** für die Wirtschaft
- NIS2-Richtlinie grundsätzlich anwendbar auf **öffentliche und private Einrichtungen**, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben – mit Ausnahmen und Einschränkungen für den öffentlichen Bereich
- **qualitative** (Anhang I und Anhang II) sowie **quantitative Konkretisierung** der betroffenen Unternehmen
- Mitgliedstaaten erstellen bis zum 17.04.2025 eine Liste wesentlicher und wichtiger Einrichtungen, die Domänennamen-Registrierungsdienste erbringen

- **Grundsatz der Mindestharmonisierung**

Was gilt bereits jetzt?

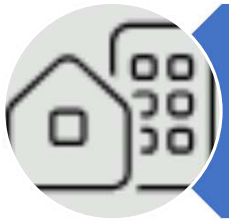
Inhalt der NIS2-Richtlinie

Bisherige KRITIS-Unternehmen

Diese Unternehmen müssen bestimmte Schwellenwerte überschreiten, um als KRITIS-Betreiber eingestuft zu werden. Ein typischer Schwellenwert ist die Versorgung von mindestens 500.000 Einwohnern.

Wesentliche / besonders wichtige Einrichtungen

Großunternehmen mit mehr als 250 Mitarbeitern fallen in diese Kategorie. Ebenso gehören Unternehmen mit einem Jahresumsatz von mindestens 50 Millionen Euro dazu. Auch Unternehmen mit einer Bilanz von mindestens 43 Millionen Euro fallen darunter.



Wichtige Einrichtungen

Mittlere Unternehmen mit mehr als 50 Mitarbeitern werden als wichtige Einrichtungen betrachtet. Ebenso gehören Unternehmen mit einem Jahresumsatz von mindestens 10 Millionen Euro in diese Kategorie. Auch Unternehmen mit einer Bilanz von mindestens 10 Millionen Euro fallen darunter.

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

Quelle: www.netplans.de/it-security/nis2/ (Abruf am 08.04.2025)

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

Was gilt bereits jetzt?

Inhalt der NIS2-Richtlinie

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

4. Umsetzungsproblematik

Umsetzungsproblematik

Geschäftsleitung

Geschäftsleitung gemäß § 2 Nr. 13 BSIG-E definiert als „eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist".

- Unklar ist, ob darüber hinaus auch **dienst- beziehungsweise arbeitsvertraglich vertretungsbefugte Personen** haftbar gemacht werden können

Umsetzungsproblematik

Einrichtungsarten

Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die **gesamte Geschäftstätigkeit** der Einrichtung **vernachlässigbar** sind , § 28 Abs. 3 BSIG-E.

Daten von Partner- oder verbundenen Unternehmen sind **nicht** hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse **unabhängig** von seinen Partner- oder verbundenen Unternehmen ist, § 28 Abs. 4 BSIG-E.

Umsetzungsproblematik

Einrichtungsarten – BSIG-E

5. Haftung der Geschäftsleitung

Haftung der Geschäftsleitung

Status quo

Geschäftsführer stehen schon heute unter Sorgfalts-, Legalitäts- und Überwachungspflichten – verankert in § 43 GmbHG und § 93 AktG.

Daraus folgt:

- IT- und Informationssicherheit gehört **untrennbar** zur **Geschäftsführungsverantwortung**.
- Auch **ohne spezielle Regelungen** wie BSIG oder DSGVO ist ein wirksames Risikomanagement zwingend.
- Pflichtverstöße – ob fahrlässig oder vorsätzlich – können zu **persönlicher zivilrechtlicher Haftung** gegenüber der eigenen Gesellschaft führen.

Haftung der Geschäftsleitung

Änderungen in Folge von NIS2

Keine völlig neuen Pflichten durch NIS2 – aber deutliche Konkretisierung und Verschärfung

- **Geschäftsleitung trägt ausdrücklich Verantwortung für Cybersicherheit**: Zustimmung, Kontrolle und Sicherstellung der Maßnahmen
- **Pflichtfortbildung**: Geschäftsführer müssen mindestens alle 3 Jahre Schulungen zu Cyberrisiken und Schutzmaßnahmen absolvieren
- **Haftung klarer definiert**: GmbHG/AktG bleiben Grundlage – § 38 BSIG-E schafft aber eine ausdrückliche Regelung für Cybersicherheit und erweitert die Haftung auf Organisationsformen wie Stiftungen und Vereine

Haftung der Geschäftsleitung

Konsequenzen

Unternehmen, die die Vorgaben der NIS2-Richtlinie nicht einhalten, riskieren **empfindliche Strafen** von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes.

Neben finanziellen Sanktionen drohen **erhebliche Reputationsschäden**, die das Vertrauen von Kunden und Partnern nachhaltig beeinträchtigen können.

Besonders kritisch: Wird ein Cyberangriff durch fehlende Sicherheitsmaßnahmen ermöglicht, kann die **Geschäftsführung persönlich haftbar gemacht werden** – selbst dann, wenn die Ursache auf Unachtsamkeit oder Versäumnisse der IT-Abteilung zurückzuführen ist.

Haftung der Geschäftsleitung

Konsequenzen

Die folgenden Szenarien zeigen beispielhaft, wie sich **mangelhafte Schutzvorkehrungen** auswirken können:

- In der IT-Infrastruktur bestehen **Schwachstellen**, die über längere Zeit nicht behoben wurden und Angreifern als Einfallstor dienten.
- Das Unternehmen hat keine angemessenen **Mitarbeiterschulungen** zur Cybersicherheit durchgeführt, weshalb Angreifer mit einer Phishing-Attacke Erfolg hatten.
- Es ist keine angemessene **Risikobewertung** oder Sicherheitsüberprüfung der eingesetzten Systeme erfolgt, wodurch Datenlecks entstanden und Informationen in die falschen Hände geraten sind.

Besonders kritisch können solche Fehler für verantwortliche Personen werden, wenn man ihnen **grobe Fahrlässigkeit** oder sogar **Vorsatz** nachweisen kann.

Haftung der Geschäftsleitung

Absicherung

Um die Haftung zu minimieren, sollten Geschäftsführer und IT-Verantwortliche deshalb eine Reihe von Maßnahmen ergreifen:

- **Schulungen anbieten und wahrnehmen**: Alle Mitarbeiter inklusive der Geschäftsführung müssen regelmäßig an Datenschutzschulungen teilnehmen, um über die neuesten Cyberbedrohungen und Sicherheitslösungen informiert zu sein.
- **Audits durchführen lassen**: Regelmäßige Sicherheitsaudits sorgen dafür, dass Schwachstellen frühzeitig identifiziert und effektiv behoben werden können.

Haftung der Geschäftsleitung

Absicherung

- Sicherheitslösungen etablieren: Unternehmen sollten in geeignete Netzwerksicherheits- und Datenschutzsoftware investieren, die den aktuellen Bedrohungen gewachsen ist.
- Up to date bleiben: Damit im Unternehmen ausreichend Know-how vorhanden ist, um Cyberangriffe abzuwehren, empfiehlt es sich, neben Schulungen auf die Zusammenarbeit mit externen Experten und Datenschutzbeauftragten zu setzen. So stellen Unternehmen sicher, dass sie neben der NIS2 auch andere Richtlinien wie die DSGVO korrekt umsetzen.

6. Fazit

Fazit

Für Geschäftsführer besteht bereits heute die Pflicht, ein angemessenes Niveau an IT- und Informationssicherheit sicherzustellen. Die NIS2-Richtlinie macht diese Verantwortung künftig transparenter, überprüfbarer und rechtlich verbindlicher. Unternehmen, die Informationssicherheit weiter vernachlässigen, riskieren nicht nur hohe Sanktionen, sondern auch eine persönliche Inanspruchnahme der Geschäftsleitung.

Vielen Dank.

Aulinger

Ihr Ansprechpartner

Dr. Ralf Heine M.M.
Rechtsanwalt | Partner
Fachanwalt für Arbeits- und IT-Recht

+49 201 9598648
+49 201 9598699
ralf.heine@aulinger.eu

Aulinger Bochum
Josef-Neuberger-Straße 4
44787 Bochum

Aulinger Essen
Frankenstraße 348
45133 Essen