

Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XV
Herausgeber- und Autor:innenverzeichnis	XXI
Literaturverzeichnis	XXV
Das NISG 2026 – Eine Einführung (Katharina Gradischnig/Felix Krysa)	1
I. Einleitung	1
II. Bisherige Rechtslage: die NIS-1-Richtlinie und das NISG	2
A. NIS-1-Richtlinie	2
B. NISG	3
1. Der sachliche Anwendungsbereich des NISG	4
a. Betreiber wesentlicher Dienste	4
b. Anbieter digitaler Dienste	6
c. Einrichtungen der öffentlichen Verwaltung	6
2. Die Verpflichtungen gem §§ 16 ff NISG	7
a. Pflichten für Betreiber wesentlicher Dienste	7
b. Pflichten für Anbieter digitaler Dienste	9
c. Pflichten für Einrichtungen der öffentlichen Verwaltung	10
3. Cyberkrise und Koordinationsausschuss	11
4. Verwaltungsstrafbestimmungen	12
5. Zwischenfazit	12
III. Die NIS-2-Richtlinie und das NISG 2026	13
A. Der sachliche Anwendungsbereich des NISG 2026	14
1. Die Sektoren	14
2. Bestimmung der Schwellenwerte	15
3. Unionsbezug	15
4. Wesentliche und wichtige Einrichtungen	16
B. Der Pflichtenkatalog des NISG 2026	16
1. Pflichten der Mitgliedstaaten	16
2. Pflichten der Einrichtungen	17
a. Risikomanagementmaßnahmen	17
b. Berichtspflicht	19
c. Aufsicht, Durchsetzung und Sanktionen	19
IV. Unterschiede NIS-1-Regulierung und NISG 2026	20
A. Ausdehnung des sachlichen Anwendungsbereichs	21
B. Wesentliche und wichtige Einrichtungen als Adressaten des NISG 2026	21

Inhaltsverzeichnis

C. Pflichtenprogramm und dessen Ausgestaltung durch das NISG 2026	22
D. Aufsicht und Durchsetzung	23
V. Fazit	24
Grundrechtliche Perspektiven (Konrad Lachmayer)	25
I. Von polizeilicher Cyberabwehr zur IT-Sicherheit	25
A. Problemstellungen sicherheits- und kriminalpolizeilicher Cyberabwehr	25
B. Regulatorische IT-Sicherheit	27
II. Grundrechtliche Rahmenbedingungen im Mehrebenensystem	29
A. Grundrechte im Mehrebenensystem	29
B. Grundrechtsverpflichtete und Grundrechtsträgerschaft	30
1. Grundrechtsverpflichtete	31
2. Grundrechtsträgerschaft	32
III. Involvierte Unternehmen und behördliche Maßnahmen	33
A. Das Grundrechtsbekenntnis der NIS-2-RL	33
B. Involvierte Unternehmen	34
C. Unternehmensbezogene Verpflichtungen und Aufsichtsmaßnahmen	35
IV. Betroffene Grundrechte	36
A. Schutz des Eigentums	36
B. Schutz der Privatsphäre im Allgemeinen	38
C. Datenschutz im Besonderen	39
D. IT-Sicherheit als Grundrecht?	41
E. Gleichheit vor dem Gesetz	42
F. Verbot der Selbstbezichtigung	44
G. Verfahrensgrundrechte	46
V. Schlussfolgerungen	47
Der Anwendungsbereich des NIS-2-Cybersicherheitsrechts (Lukas B. Wieser)	49
I. Vom Nischenthema zur „Chefsache“	49
II. Anwendungsbereich im Überblick	51
III. Die Sektoren der Anhänge I und II	53
A. Allgemeines	53
B. Anhang I	55
1. Energie (Nr 1 Anhang I)	55
2. Verkehr (Nr 2 Anhang I)	56
3. Bankwesen (Nr 3 Anhang I)	57

Inhaltsverzeichnis

4. Finanzmarktinfrastrukturen (Nr 4 Anhang I)	57
5. Gesundheitswesen (Nr 5 Anhang I)	57
6. Trinkwasser (Nr 6 Anhang I)	58
7. Abwasser (Nr 7 Anhang I)	58
8. Digitale Infrastruktur (Nr 8 Anhang I)	59
9. Verwaltung von IKT-Diensten (Business-to-Business) (Nr 9 Anhang I)	60
10. Öffentliche Verwaltung (Nr 10 Anhang I)	60
11. Weltraum (Nr 11 Anhang I)	61
C. Anhang II	62
1. Post- und Kurierdienste (Nr 1 Anhang II)	62
2. Abfallbewirtschaftung (Nr 2 Anhang II)	62
3. Produktion, Herstellung und Handel mit chemischen Stoffen (Nr 3 Anhang II)	63
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Nr 4 Anhang II)	64
5. Verarbeitendes Gewerbe/Herstellung von Waren (Nr 5 Anhang II)	65
6. Anbieter digitaler Dienste (Nr 6 Anhang II)	66
7. Forschung (Nr 7 Anhang II)	66
IV. Große und mittlere Unternehmen	67
A. Die Größenklassen der KMU-Empfehlung	67
B. Zurechnung von verbundenen und Partnerunternehmen	68
1. Regel: Konsolidierung im Konzern	68
2. Ausnahme: Keine Zurechnung bei organisatorischer, technischer und operativer Unabhängigkeit (§ 25 Abs 4 NISG 2026)	69
V. Größenunabhängige Anwendung	71
A. Allgemeines	71
B. Ausübung einer spezifischen Tätigkeit/Tätigkeit in einem spezifischen (Teil-)Sektor	71
C. Systemische Bedeutung	72
VI. Prüfschema Anwendungsbereich	74
 Zum Schutzgut des Cybersicherheitsrisikomanagements iSd Art 21 der NIS-2-RL (Boris Trembl)	
I. Einleitung und Gang der Untersuchung	75
II. Die Entstehung des modernen IT-Sicherheitsrechts vom Politikansatz zur NIS-Regulierung	76

Inhaltsverzeichnis

III. Die Schutzgüter des Cybersicherheitsrisikomanagements	80
A. Das NIS im Detail	81
1. Elektronisches Kommunikationsnetz	81
a. Übertragungssystem	81
b. Stromleitungssysteme	83
c. Netze für Hör- und Fernsehfunksowie Kabelfernsehnetze	84
d. Der Begriff des elektronischen Kommunikationsnetzes	84
2. Das Gerät als Bestandteil des NIS	84
3. Digitale Daten als Bestandteil des NIS	85
4. Abschließende Betrachtung des NIS	86
a. Berücksichtigung Strafrechtsrichtlinie	86
b. Abschließende Betrachtung	88
B. Das Schutzgut von der NIS-1-RL zur NIS-2-RL	89
C. Die Bedeutung des IKT-Dienstes, -Produktes und -Prozesses	90
D. Auslegung des NIS-2-Schutzgutes im Lichte der DORA	91
E. Zum Schutzziel der DORA	91
IV. Fazit	94

Lieferkettensicherheit gemäß der NIS-2-RL *(Christoph Reiter/ Marcus Luser)*

I. Die Bedeutung von Cybersicherheit in der Lieferkette	97
II. Normative Grundlagen	98
III. Lieferkettensicherheit als vertragliche Realität – Notwendigkeit der Umsetzung im Vertragsbestand	99
A. NIS-2 – Analyse bestehender Lieferantenverträge, Informationspflichten des Lieferanten?	101
1. Vertragliche Neben(leistungs)plichten	101
a. Selbstständige Nebenleistungspflichten	102
b. Unselbstständige Nebenleistungspflichten	103
c. Schutz- und Sorgfaltspflichten	103
d. Rechtsfolgen bei Verletzung vertraglicher Neben(leistungs)plichten	103
2. Informationspflicht des Lieferanten als vertragliche Neben(leistungs)plicht?	104

Inhaltsverzeichnis

B. Einseitige Anpassung bestehender Lieferantenverträge?	106
1. Vertragsanpassung wegen Irrtums?	106
a. Allgemeines	106
b. Voraussetzungen für eine Vertragsanpassung wegen Irrtums	107
aa. Beachtlichkeit des Irrtums	107
bb. Kausalität und Wesentlichkeit des Irrtums	108
cc. Vorliegen einer der Alternativvoraussetzungen des § 871 ABGB	109
c. Einseitige Anpassung von Lieferantenverträgen wegen Irrtums in Bezug auf NIS-2?	110
2. Vertragsanpassung wegen Wegfalls der Geschäftsgrundlage?	111
a. Allgemeines zur Lehre vom Wegfall der Geschäftsgrundlage	111
b. Konkrete Tatbestandsvoraussetzungen	112
aa. Fehlen oder Wegfall einer Geschäftsgrundlage	112
bb. Weitere Voraussetzungen	113
c. Rechtsfolgen bei Wegfall der Geschäftsgrundlage	114
d. Einseitige Anpassung von Lieferantenverträgen wegen Wegfalls der Geschäftsgrundlage durch Inkrafttreten von NIS-2?	115
3. Verhandlungspflicht und Kontrahierungszwang des Vertragspartners?	116
a. Ergänzende Vertragsauslegung	116
aa. Allgemeines zur ergänzenden Vertragsauslegung	116
bb. Verhandlungspflicht und Kontrahierungszwang als Resultat ergänzender Vertragsauslegung?	117
b. Verhandlungspflicht und Kontrahierungszwang zur Umsetzung von NIS-2?	118
4. Fazit	121
C. Ultima ratio – Vertragsauflösung	121
1. Außerordentliche Kündigung von Dauerschuldverhältnissen	122
a. Allgemeines zur (außer-)ordentlichen Kündigung	122
b. Voraussetzungen für eine außerordentliche Kündigung	123
aa. Wichtiger Kündigungsgrund	123
bb. Rechtzeitige Geltendmachung	124
c. Rechtsfolgen einer außerordentlichen Kündigung	125
d. Exkurs: Verhältnis zum Institut des Wegfalls der Geschäftsgrundlage	125

Inhaltsverzeichnis

2. Außerordentliche Kündigungsmöglichkeit iZm der NIS-2-RL	126
IV. Fazit und Ausblick	128
Deliktische Haftung bei Verstößen gegen die NIS-2-Regelungen?	
<i>(Roman Heidinger)</i>	131
I. Einleitung	131
II. Abgrenzung zur Vertragshaftung und Haftung von Organen gegenüber der Gesellschaft	132
III. Datenschutzverletzungen als Sonderfall	133
IV. Deliktische Haftung für Cybersicherheitsvorfälle nach allgemeinen zivilrechtlichen Grundsätzen	133
A. Allgemeines	133
B. Haftung wegen Eingriffs in absolut geschützte Rechtsgüter	135
C. Haftung wegen Schutzgesetzverletzung	139
D. Problematik der Gehilfenzurechnung	142
V. Zusammenfassung	143
Cybersicherheitsrechtliches Verwaltungshandeln	
<i>(Eleonóra Wagenknecht)</i>	145
I. Einleitung	145
II. Zuständige Behörden	146
A. Bisheriges Konzept	146
B. Änderungen durch die NIS-2-RL und das NISG 2026	148
1. Allgemeines	148
a. Behörden	148
b. Betroffene Einrichtungen	149
2. Aufsichts- und Durchsetzungsmaßnahmen	149
a. Aufsichtsmaßnahmen	149
aa. Maßnahmen gegenüber wesentlichen Einrichtungen	149
bb. Maßnahmen gegenüber wichtigen Einrichtungen	151
b. Durchsetzungsmaßnahmen	152
aa. Generelle Maßnahmen	152
bb. Maßnahmen gegenüber wesentlichen Einrichtungen im Besonderen	153
III. Computer-Notfallteams	153
A. Bisheriges Konzept	153
B. Änderung durch die NIS-2-RL und das NISG 2026	154
C. Beleihung von CERT.at	155

Inhaltsverzeichnis

IV. Einordnung des Verwaltungshandelns und Rechtsschutz	158
A. Allgemeines	158
B. Cybersicherheitspolizei	158
C. Cybersicherheitsrechtliche Hoheitsverwaltung	161
1. Bescheide	161
2. Akte unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt (AuvBZ)	161
3. Schlichte Hoheitsverwaltung	162
D. Rechtsschutzdefizit	163
V. Fazit	164
Stichwortverzeichnis	167

Das Streben nach Klarheit und Lesbarkeit veranlasst uns dazu, im Text auf die gleichberechtigte Nennung aller Geschlechter zu verzichten. Sämtliche personenbezogene Hauptwörter beziehen sich gleichermaßen auf die Entsprechungen anderer Geschlechter.