HEUKING KÜHN LÜER WOJTEK

NIS2-Richtlinie und IT-Sicherheitsgesetz 3.0: Was Unternehmen jetzt für ihre Cybersicherheit tun müssen

Fachkonferenz Cybersicherheit

09.11.2023

Dr. Lutz M. Keppeler

Fachanwalt für IT-Recht

RECHTSANWÄLTE UND STEUERBERATER

Das IT-Sicherheitsrecht „bisher“

I. Was gibt es jetzt schon an IT-Sicherheits Recht

- IT Sicherheitsgesetz (2015) => Erstmals gebündelte Spezialregelungen für KRITIS Betreiber
- NIS-Richtlinie 2017 (Für Deutschland neu nur die Regeln über „ Regelungen für Anbieter digitaler Dienste“)
- DSGVO 2018, insbesondere Art 32 DSGVO und Art 82 DSGVO
- IT-Sicherheitsgesetz 2.0 (Mehr Kompetenzen für das BSI, Ausweitung der KRITIS Regelungen, „Lex Huawei“; Regeln für „Unternehmen im besonderen öffentlichen Interesse“)
- Nicht zu vergessen: Dass allgemeine Zivilrecht

I. Bislang wenige Detailvorgaben im IT-Sicherheitsrecht

- Z.B: Art. 32 DSGVO:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“*

- Problem des IT-Sicherheitsrechts: „Technikneutrale Formulierung“

I. Der Gesetzgeber regelt aber keinen konkreten Details

- Müssen Daten während der Übertragung und während der Speicherung verschlüsselt werden ?
  - Wenn ja, wie stark?
- Benötigt ein Unternehmen ein ISMS („Information Security Management System“)?
- Wie lang muss ein Passwort sein und welche Merkmale muss es aufweisen?
- Wie häufig muss man IT-Sicherheitsupdates liefern?
- Benötigt mein Produkt/meine IT-Umgebung ein „Intrusion detection system“?
- Genügt eine x-beliebige Firewall, oder kommt es auf die spezifische Parametrisierung an?
- Müssen Angestellte geschult werden? Wenn ja, nach welchem Inhalt, wie regelmäßig?
- Muss man einen Penetrationstest durchführen und wenn ja, wie intensiv und wie häufig zu wiederholen?
- Müssen Software Bill of Material mitgeliefert werden?

I. Vergleich zur Entwicklung des Automobilrechts

Beginn: Ohne jede Regel; unklar wer haftet

Automobil nach „mittlerer Art und Güte“

Heute: Viele Detailregelungen

- Blinker
- Airbag
- Sicherheitsgurt…

- Sogar mittlerweile Detailvorgaben zur IT-Sicherheit

Das Problem der Generalklauseln

Die EU-Digitalstrategie

II. Einordnung der Rechtsakte der EU

Gestaltung der digitalen Zukunft Europas: Die EU Digitalstrategie bis 2030

↓

Schlussfolgerungen zur Cybersicherheitsstrategie der EU

- Resilienz, technologische Souveränität und Führungsrolle
- Aufbau operativer Kapazitäten zur Verhinderung, Abschreckung und Reaktion
- Förderung eines globalen und offenen Cyberspace durch verstärkte Zusammenarbeit

Umsetzung in Rechtsakten:

Organisationen	Produkte und Dienstleistungen
NIS-2-Richtlinie	Cyber Resilience Act
CER-Richtlinie	Data Act
Digital Operational Resilience Act	Data Governance Act
Cyber Solidarity Act	Artificial Intelligence Act

II. Gesetzgebungen im Rahmen der EU Digitalstrategie (Auszug)

	Aktueller Stand	Sanktionen
Digital Services Act	In Kraft getreten am 16. November 2022, gilt ab **17. Februar 2024**	bis zu 6 % des Jahresumsatzes für Verstöße sehr großer Online-Plattformen; im Übrigen sollen Mitgliedstaaten Sanktionen festlegen
Digital Markets Act	In Kraft getreten am 1. November 2022, gilt ab **02. Mai 2023**	bis zu 10 % des Jahresumsatzes
Data Act	Politische Einigung zwischen dem Europäischen Parlament und dem Rat der EU am 28. Juni 2023	Mitgliedstaaten sollen Sanktionen festlegen.
Data Governance Act	In Kraft getreten, ab dem **24. September 2023** anwendbar	"Abschreckende Geldstrafen"
Cyber Resiliance Act	Entwurf vom 15. September 2022; Kompromisstext des Rates der EU liegt seit dem 15. Juni 2023 vor; Beginn des Trilogs voraussichtlich September 2023 und in Kraft treten in 2024 angestrebt	15 Mio. Euro oder 2,5 % des weltweiten Jahresumsatzes
NIS-2-Richtlinie	In Kraft getreten; Umsetzungsfrist **07. Oktober 2024**	Für wesentliche Einrichtungen 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes
AI Regulation	Annahme des Gesetzesentwurfes am 14. Juni 2023; Beginn des Trilogs	maximal 30 Mio. Euro oder 6 % des weltweiten Jahresumsatzes
Richtlinie über KI-Haftung	Entwurf **28.09.2022**	Keine
Digital Operational Resilience Act (DORA)	In Kraft getreten am 16. Januar 2023; Anwendbar ab **17. Januar 2025**	Sanktionen sollen von Mitgliedsstaaten festgelegt werden
European Health Data Space (Regulation)	Entwurf vom **03.05.2022**	Sanktionen sollen von Mitgliedsstaaten festgelegt werden

II. CRA -Pflichtenkatalog (Auszug)

Hersteller

- Prozess- und Dokumentationspflichten
- Cybersicherheits-Risikoanalyse zu Produktrisiken
- Durchführung eines Konformitätsbewertungsverfahrens zur Produkteinstufung
- Erstellung der technischen Dokumentation
- Verfahrens- und Informationspflichten
- Informations- und Meldepflichten bei Schwachstellen

Einführer

- Überprüfungspflichten vor Import
- CE-Kennzeichnung und technische Dokumentation
- Ergänzung eigener Firmenname oder Marke sowie Kontaktinformationen auf dem Produkt
- Aufbewahrungspflicht
- Informationspflicht ggü. Hersteller bei Feststellung von Schwachstellen

Händler

- Überprüfungspflichten vor Bereitstellen auf dem Markt
- CE-Kennzeichnung, technische Dokumentation und Gebrauchsanweisung
- Informationspflicht gegenüber Hersteller bzw. nationalen Marküberwachungsbehörden bei Feststellung von Schwachstellen

II. CRA Pflichtenkatalog gemäß Anlage 1

- Produkte mit digitalen Elementen müssen ohne bekannte ausnutzbare Schwachstellen geliefert werden.
- Auf der Grundlage einer verpflichtenden Risikobewertung müssen Produkte mit digitalen Elementen:
  - die Verfügbarkeit wesentlicher Funktionen schützen, einschließlich der Widerstandsfähigkeit gegen und der Abschwächung von Denial-of-Service-Angriffen
  - sicherheitsrelevante Informationen durch Aufzeichnung und/oder Überwachung relevanter interner Aktivitäten speichern („Logfiles“)
- Hersteller sind zur „Marktüberwachung“ bzgl. IT-Sicherheit verpflichtet
- Informationspflichten zur Cybersicherheit gegenüber dem Nutzer („Beipackzettel“)
- Zurverfügungstellung von „Software Bill of Materials“ (umstritten!)
  - Details über alle Komponenten und „Lieferkette“

II. Wording (Auszug)

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that ~~exploitable~~ vulnerabilities are fixed or mitigated in a timely **and, where applicable, automatic** manner;

Die NIS-2 Richtlinie und NIS2UmsuCG (Entwurf)

II. NIS-2-Richtlinie und NIS2UmsuCG – Wesentliche Inhalte

NIS-2-Richtlinie

- Adressaten sind „**wesentliche“ und „wichtige Einrichtungen“**, die ihre Dienste in der EU erbringen oder Tätigkeit dort ausüben.
- Ziel ist die Sicherstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU.
- Einordnung als wesentliche oder wichtige Einrichtung richtet sich nach mehreren Faktoren
- Wesentliche Pflichten betreffen Governance-Vorgaben an die Geschäftsleitung, Umsetzung von Risikomanagementmaßnahmen, Melde- und Berichtspflichten
- Hohe Bußgelder bei Pflichtverletzungen
- Umsetzung in Deutschland: NIS2UmsuCG bzw. IT-Sicherheitsgesetz 2024

NIS2UmsuCG (Entwurf)

- Adressaten sind „**wichtige**“ und „**besonders wichtige Einrichtungen**“ sowie „**Betreiber kritischer Anlagen“.**
- Betreiber kritischer Anlagen sind automatisch wesentliche Einrichtungen im Sinne der NIS-2-Richtlinie.
- Umsetzung der Governance-Vorgaben an die Geschäftsleitung, Umsetzung von Risikomanagementmaßnahmen, Melde- und Berichtspflichten
- Hohe Bußgelder bei Pflichtverletzungen

II. NIS-2-Richtlinie und NIS2UmsuCG - Schwellwerte

NIS-2-Richtlinie

Groß:

Müssen den Schwellenwert für „mittlere Unternehmen“ überschreiten, d.h.:

> 249 Mitarbeiter und > 50 Mio. EUR Jahresumsatz oder > 43 Mio. EUR Jahresbilanzsumme

Mittel: Müssen den Schwellenwert für „mittlere Unternehmen“ einhalten, d.h.:

50-249 Mitarbeiter und 10-50 Mio. EUR Jahresumsatz oder 10-43 Mio. EUR Jahresbilanzsumme

NIS2UmsuCG (Entwurf)

Groß:

Müssen den Schwellenwert für „mittlere Unternehmen“ überschreiten, d.h.:

> 249 Mitarbeiter oder > 50 Mio. EUR Jahresumsatz und zudem > 43 Mio. EUR Jahresbilanzsumme

Mittel:

50-249 Mitarbeiter und weniger als 50 Mio. EUR Jahresumsatz oder weniger als 43 Mio. EUR Jahresbilanzsumme (**derzeit keine Untergrenzen vorgesehen!**)
oder
weniger als 50 Mitarbeiter und Jahresumsatz zwischen 10 Mio. EUR und 50 Mio. EUR und Jahresbilanzsumme zwischen 10 Mio. EUR und 43 Mio. EUR.

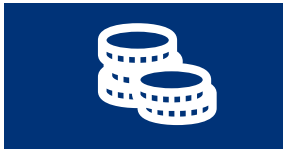
Ablösung bisheriges Konzept der Schwellwerte???

II. NIS-2-Richtlinie und NIS2UmsuCG – Übersicht der Sektoren

Anhang I: Sektoren mit hoher Kritikalität


Energie


Verkehr

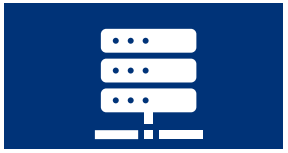

Bankwesen


Finanzmarktinfrastruktur


Gesundheitswesen


Trinkwasser


Abwasser


Digitale Infrastruktur


Verwaltung von IKT-Diensten


Öffentliche Verwaltung


Weltraum

Anhang II: Sonstige Kritische


Post- und Kurierdienste


Abfallwirtschaft


Produktion, Herstellung und Handel mit chemischen Stoffen


Produktion, Verarbeitung und Vertrieb von Lebensmitteln


Verarbeitendes Gewerbe/Herstellung von Waren


Anbieter digitaler Dienste


Forschung

II. NIS-2-Richtlinie und NIS2UmsuCG – Übersicht der Sektoren

Größenunabhängige wesentliche Einrichtungen

- Qualifizierte Vertrauensdienste-anbieter
- TLD-Anbieter der obersten Stufe
- DNS-Diensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder -dienste
- Einrichtungen öffentlicher Verwaltung der Zentralregierung
- Kritische Einrichtungen gemäß CER-RL
- Betreiber wesentliche Dienste gemäß RL 2016/1148 (vor 16.01.2023)
- Sonstige nach nationale Recht eingestufte Einrichtungen (Anhang I oder II)

Größenunabhängige wichtige Einrichtungen

- Nach nationalem Recht eingestufte Einrichtungen (Anhang I oder II + Kriterien zur Kritikalität in Art. 2 Abs. 2 lit. b bis e)

II. NIS-2-Richtlinie und NIS2UmsuCG – Governance-Pflichten

Pflichten der Geschäftsleitung

- Pflicht zur Einführung, Billigung und Überwachung der Umsetzung der Risikomanagementmaßnahmen
- Pflicht zur Teilnahme an Schulungen im Bereich Cybersicherheit.

Sanktionen gegenüber Geschäftsleitung

- Persönliche Haftung: Leitungspersonal soll für Verstöße gegen Governance-Pflichten verantwortlich sein
- Befugnis der Behörden zur vorübergehenden Untersagung der Wahrnehmung von Leitungsaufgaben, falls Durchsetzungsmaßnahmen nicht oder nicht wirksam umgesetzt werden (nur bei wesentlichen Einrichtungen!)

Geplante Umsetzung in Deutschland

- Persönliche Haftung für Schäden gegenüber der Einrichtung (ohne Möglichkeit auf Verzicht oder Vergleich)
- Schadensbegriff soll Regressansprüche und **Bußgeldforderungen** erfassen

Konsequenz: Cyber-Security ist Aufgabe der Geschäftsleitung!

II. NIS-2-Richtlinie und NIS2UmsuCG – Governance-Pflichten

Risikomanagementmaßnahmen

- Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige **technische**, **operative und organisatorische Maßnahmen** ergreifen, um Risiken für die Sicherheit der eingesetzten Netz- und Informationssysteme zu beherrschen und Auswirkungen von Sicherheitsvorfällen zu verhindern oder zumindest möglichst gering zu halten.

Risikobetrachtung

- Berücksichtigung des **Standes der Technik**, ggfs. europäischer oder internationale Normen sowie Kosten der Umsetzung, um ein dem Risiko **angemessenes Sicherheitsniveau** zu gewährleisten. Die Umsetzung der Maßnahmen muss auf einem gefahrübergreifendem Ansatz beruhen.

Verhältnismäßigkeit

- Bei der Bewertung der Verhältnismäßigkeit sind **verschiedene Faktoren** zu beachten (u.a. Risikoexposition und Größe der Einrichtung, Wahrscheinlichkeit und Folgen von Sicherheitsvorfällen).

II. NIS-2-Richtlinie und NIS2UmsuCG – Risikomanagement

Risikomanagementpflichten

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (**Sicherheitskonzepte**)
- Maßnahmen zur **Bewältigung von Sicherheitsvorfällen**
- Maßnahmen zur **Aufrechterhaltung des Betriebs** (Backup-Management und die Notfall-Wiederherstellung von Daten, Krisenmanagement)
- **Sicherheit der Lieferkette** und Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen (einschließlich Management und Offenlegung von Schwachstellen)
- Konzepte und Verfahren zur **Bewertung der Wirksamkeit der Risikomanagementmaßnahmen** im Bereich Cybersicherheit
- Grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggfs. **Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und Management von Anlagen
- **Verwendung von Lösungen zur Multi-Faktor-Authentifizierung** oder kontinuierlichen **Authentifizierung**, **gesicherte Sprach-, Video- und Text-Kommunikation** sowie ggfs. gesicherte **Notfallkommunikationssysteme**

II. NIS-2-Richtlinie und NIS2UmsuCG – Aufsicht und Durchsetzung

- Gestuftes Konzept für wesentliche und wichtige Einrichtungen
- Zusammenarbeit von Datenschutz-Aufsichtsbehörden und Cybersicherheits-Behörden vorgesehen.
- Rangfolge: Erst Aufsichtsmaßnahmen; dann Durchsetzungsmaßnahmen; danach ggfs. Sanktionen.

Aufsichtsmaßnahmen

- Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen (einschl. Stichprobenkontrollen)
- Regelmäßige und gezielte Sicherheitsprüfungen
- Ad-Hoc-Prüfungen im Zusammenhang mit erheblichen Sicherheitsvorfällen oder Verstößen
- Sicherheitsscans
- Anforderung von Informationen und Nachweisen zur Umsetzung von Cybersicherheitskonzepten (z.B. Ergebnisse von Sicherheitsprüfungen)

Durchsetzungsmaßnahmen

- Warnungen über Verstöße
- Erlass von verbindlichen Anweisungen und Anordnungen
- Benennung eines Überwachungsbeauftragten

Nur bei wesentlichen Einrichtungen:

- Vorübergehende Aussetzung der Zertifizierung oder Genehmigung für von der Einrichtung erbrachten Dienste oder Tätigkeiten
- Zeitweise Untersagung der Ausübung von Leitungsaufgaben von Mitgliedern der Geschäftsführer-, bzw. Vorstandsebene durch hierfür zuständige Stellen oder Gerichten

II. NIS-2-Richtlinie und NIS2UmsuCG – Aufsicht und Durchsetzung

Sanktionen

- Bußgelder sollen wirksam, verhältnismäßig und abschreckend sein
- Berücksichtigung von verschiedene Faktoren bei Verhängung von Bußgeldern (z.B. Schwere und Dauer des Verstoßes, frühere Verstöße, verursachte Schäden, Vorsatz oder Fahrlässigkeit, ergriffene Maßnahmen zur Verhinderung und Minderung von Schäden, Zusammenarbeit mit Behörden)

Voraussetzungen

- Verstoß gegen Pflicht zur Teilnahme an Schulungen im Bereich Cybersicherheit.
- Fehlende oder unzureichende Umsetzung der erforderlichen Risikomanagementmaßnahmen
- Verletzung der Berichtspflichten

Erhebliche Erhöhung des Bußgeldrahmensbliche

- Bei wesentlichen Einrichtungen: Bis zu 10 Mio. EUR bzw. 2 %*
- Bei wichtigen Einrichtungen: Bis zu 7 Mio. EUR bzw. 1,4 %*
- Aktuell beträgt der Bußgeldrahmen bis zu 2 Mio. EUR

*des gesamten weltweiten Jahresumsatzes (je nach Verstoß und je nachdem, welcher Betrag höher ist)

II. CER-Richtlinie und KRITIS-DachG – Vergleich zur NIS-2-Richtlinie

NIS-2-Richtlinie

- Adressaten sind **wesentliche und wichtige Einrichtungen**, die ihre Dienste in der EU erbringen oder Tätigkeit dort ausüben.
- Ziel ist die Sicherstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU.
- Einordnung als wesentliche oder wichtige Einrichtung richtet sich nach mehreren Faktoren
- Wesentliche Pflichten betreffen **Governance-Vorgaben** an die Geschäftsleitung, Umsetzung von **Risikomanagementmaßnahmen**, **Melde- und Berichtspflichten**
- Umsetzung in Deutschland: NIS2UmsuCG bzw. IT-Sicherheitsgesetz 2024

CER-Richtlinie

- Adressaten sind **Betreiber kritischer Anlagen**. Diese sind automatisch wesentliche Einrichtungen im Sinne der NIS-2-Richtlinie.
- Ziel ist die Verbesserung der (physischen) Resilienz und der Fähigkeit zur Erbringung ihrer Dienste.
- Wesentliche Pflichten betreffen die Vornahme von **Risikobewertungen**, Umsetzung von **Resilienzmaßnahmen**, **Melde- und Berichtspflichten**
- Betreiber kritischer Einrichtungen mit besonderer Bedeutung für Europa unterliegen weiteren Pflichten.
- Umsetzung in Deutschland: KRITIS-Dachgesetz

III. Fazit

- Stand jetzt hilft einem der Gesetzgeber nicht!
  - Bislang basiert das IT-Sicherheitsrecht in Deutschland auf „Generalklauseln“ (bei wenig Rechtsprechung)
  - Detailregelungen bislang nur in Verträgen

- EU-Digitalisierungsstrategie ist „Game Changer“ für das IT-Sicherheitsrecht
  - NIS-2: Persönliche Verpflichtung für Management
  - NIS-2: Detailvorgaben für Risikomanagement
  - NIS-2: Höhere Sanktionen
  - NIS-2: Ausweitung des Anwendungsbereiches
  - CRA: Hohe Cybersicherheitsanforderungen für alle vernetzten Produkte

Praxisumsetzung bleibt abzuwarten; Detailchaos bei Involvierung mehrerer Aufsichtsbehörden

Das Heuking IT-Security Kern-Team

Dr. Lutz Keppeler

Partner

- Fachanwalt für IT-Recht
- ISO 27001 Foundation

Manuel Poncza

Associate

- IT-Security-Manager (TÜV)
- IT-Security-Beauftragter (TÜV)
- IT-Compliance Manager (TÜV)

Michael Kuska

Salaried Partner

- ISO 27001 Foundation
- ISO 27001 Security Officer

Dr. Stefan Jöster

Partner

- Fachanwalt für Versicherungsrecht
- Spezialist für Cyber Versicherungen

Gebündelte Kompetenz:

- Weitere Fachanwälte für IT-Recht
- Praxisgruppe IT/IP mit über 40 Anwälten
- Langjährige Praxiserfahrung im Cyber-Strafrecht
- Kontakt zu Polizei / StA
- Kontakt zu BSI
- Kontakt zu Datenschutz-Aufsichtsbehörden
- Regelmäßig in internationalen Mandaten tätig
- Koordination von Behörden-Meldungen in allen Ländern der Welt

Ansprechpartner

Dr. Lutz M. Keppeler

Partner

Fachanwalt für IT-Recht

Magnusstraße 13

50672 Köln

T +49 221 2052-426

F +49 221 2052-1

l.keppeler@heuking.de

Kompetenzen

- IT-Recht mit Spezialisierung auf IT-Sicherheitsrecht und Open Source Lizenzen
- Datenschutzrecht
- Telekommunikationsrecht

Mitgliedschaften

- Fellow der European Free Software Foundation (FSFE)
- International Bar Association (IBA)

Veröffentlichungen (Auszug)

- Die Open-Source-Bereichsausnahme im Entwurf des Cyber-Resilience-Act Zeitschrift für Product Compliance (ZfPC) 2023, S. 117-123
- Kapitel „Cyberversicherungen“ in: Wollinger / Schulze (Hrsg.) Handbuch Cybersecurity für die öffentliche Verwaltung, 2020
- § 2, 4a,4b,5b,7a-c,9b BSIG, § 11 EnWG, § 109 TKG in Ritter, Kommentar zum IT-Sig. 2.0 (2021)
- „Datenschutz und SSL-Decryption“ K&R 2017, 453 ff.
- Technische und rechtliche Probleme bei der Umsetzung der DSGVO Löschpflichten ZD 2017, 314 ff.

HEUKING KÜHN LÜER WOJTEK

Vielen Dank
für Ihre Aufmerksamkeit

www.heuking.de

Berlin
Kurfürstendamm 32
10719 Berlin
T +49 30 88 00 97-0
F +49 30 88 00 97-99

Düsseldorf
Georg-Glock-Straße 4
40474 Düsseldorf
T +49 211 600 55-00
F +49 211 600 55-050

Hamburg
Neuer Wall 63
20354 Hamburg
T +49 40 35 52 80-0
F +49 40 35 52 80-80

München
Prinzregentenstraße 48
80538 München
T +49 89 540 31-0
F +49 89 540 31-540

Chemnitz
Weststraße 16
09112 Chemnitz
T +49 371 38 203-0
F +49 371 38 203-100

Frankfurt
Goetheplatz 5-7
60313 Frankfurt am Main
T +49 69 975 61- 0
F +49 69 975 61-200

Köln
Magnusstraße 13
50672 Köln
T +49 221 20 52-0
F +49 221 20 52-1

Stuttgart
Augustenstraße 1
70178 Stuttgart
T +49 711 22 04 579-0
F +49 711 22 04 579-44

Zürich
Bahnhofstrasse 69
8001 Zürich/Schweiz
T +41 44 200 71-00
F +41 44 200 71-01