

Factsheet

DORA – Next Level of Cyber Risk Management

Wie sich Finanzinstitute und IT-Dienstleister effektiv und umfassend auf die neuen Anforderungen des Digital Operational Resilience Act vorbereiten können!



DORA schafft neuen Rahmen für digitale Resilienz

Der Digital Operational Resilience Act (DORA) ist seit dem 16.01.2023 in Kraft und ist in allen EU-Mitgliedstaaten **ab dem 17.01.2025 verbindlich** anzuwenden. Kernziel von DORA ist die Schaffung eines EU-weiten Rechtsrahmens zur **Stärkung der Cybersicherheit und der digitalen Betriebsfestigkeit** des Finanzsektors unter Einbezug der IT-Dienstleister. DORA schafft ein Regelwerk, um angemessen auf Störungen und Bedrohungen der Informations- und Kommunikationstechnologie (IKT) zu reagieren und Cyber-Angriffe zu verhindern bzw. ihre Auswirkungen zu minimieren.

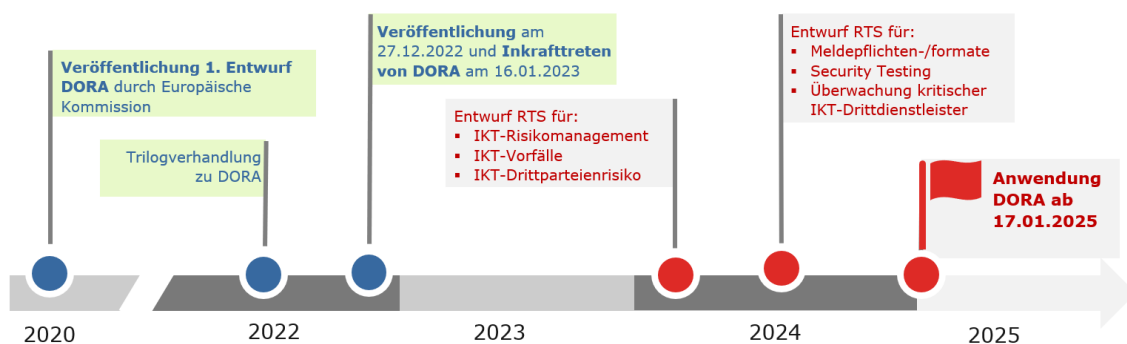


Abb.: Zeitplan der Umsetzung von DORA

Wer ist von DORA betroffen?

Der Anwendungsbereich von DORA wurde gegenüber den bisherigen europäischen und nationalen Regularien **deutlich erweitert**. Somit ist DORA grundsätzlich für **alle Kreditinstitute, Zahlungsinstitute, Versicherungsunternehmen, Investmentfirmen** sowie **IKT-Drittanbieter**, die digitale (Daten-) Dienstleistungen anbieten, anzuwenden.

Welche Herausforderungen bestehen in der Umsetzung?

- Komplexität der Regelungen:** DORA umfasst **zahlreiche technische und rechtliche Anforderungen**. Allerdings fehlen zum aktuellen Zeitpunkt teilweise noch konkrete Regulierungsstandards (RTS).
- Hohe Umsetzungs- und Betriebskosten:** Die Umsetzung von DORA erfordert **erhebliche Investitionen in IT-Infrastruktur und Sicherheitsmaßnahmen**, was für kleine und mittelständige Institute eine finanzielle Belastung darstellen kann.
- Anwendungspraxis:** Interpretationsspielräume und eine **abweichende Prüfungspraxis** erhöhen die **Unsicherheit in der Anwendung** geltender Anforderungen.
- Technologische Anpassungen:** Unternehmen müssen ihre **IT-Infrastruktur** an die DORA-Anforderungen anpassen.
- Externe Abhängigkeiten:** Die Sicherheit und Zuverlässigkeit von Dienstleistern und Infrastrukturanbietern **beeinflussen die Betriebsfestigkeit** und erfordern zukünftig eine enge Zusammenarbeit.

Überblick zu den Kernthemen von DORA

Die DORA-Vorgaben ergänzen und **erweitern die bestehenden Regularien**, wie EBA-Leitlinien zu Auslagerungen und IKT-Risikomanagement sowie die Anforderungen der MaRisk/BAIT, MaGo/VAIT und KaMaRisk/KAIT.

Die neuen Regelungen beinhalten detaillierte Anforderungen in folgenden wesentlichen Themenbereichen (siehe Abbildung). Darüber hinaus erlässt DORA neue Vorgaben, die an die Aufsichtsbehörden gerichtet sind, wie bspw. Vorgaben zu Meldungen von IKT-Sicherheitsvorfällen.

Kapitel II: IKT-Risikomanagement (Art. 5 - 16)

- ▶ Erweiterte Pflichten des Managements
- ▶ Etablierung einheitlicher Vorgaben zu Erkennung von und Reaktion auf IKT-Störungen
- ▶ Vereinheitlichung des IKT-Risikomanagement-Rahmens inkl. Richtlinien, Anweisungen und Prozessen
- ▶ Verwendung von IKT-Sicherheitstools, -Richtlinien und -Verfahren
- ▶ Spezifizierung von Notfallplänen zur Reaktion und Wiederherstellung

Kapitel III: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Art. 17 - 23)

- ▶ Standardisierte Überwachung von Cyber-Bedrohungen
- ▶ Einführung eines Frühwarnsystems
- ▶ Klassifizierung aller IKT-Vorfälle sowie deren umfassende Auswirkungsanalyse
- ▶ Erweiterte Aufzeichnungspflichten
- ▶ Vordefinition von Kommunikationsplänen
- ▶ Erweiterte Meldepflichten von schwerwiegenden IKT-Vorfällen

Kapitel V: Management des IKT-Drittparteirisikos (Art. 28 - 44)

- ▶ Pflege eines Informationsregisters (inkl. IT-Fremdbezüge)
- ▶ Zusätzliche Anforderung an die Überwachung von IKT-Drittdienstleister Risiken
- ▶ Risikoanalysen und Ausstiegsstrategien (auch für IT-Fremdbezüge)
- ▶ Stärkere Überwachung und Analyse von Weiterverlagerungen
- ▶ Weitreichende Prüfungsrechte der Aufsichtsbehörden

Kapitel IV: Testen der digitalen operationalen Resilienz (Art. 24 - 27)

- ▶ Erweiterte Anforderungen an das Testprogramm zur Prüfung der digitalen Betriebsstabilität (Penetration Testing)
- ▶ Überprüfung kritischer Funktionen & Dienstleistungen inkl. Auslagerungen
- ▶ Erweitertes Spektrum geeigneter Tests inkl. konkreter Testverfahren
- ▶ Beauftragung externer Dienstleister für Thread Led Penetration Tests (TLPT)
- ▶ Nachweispflicht der Qualifikationen interner und externer Prüfer/ Tester
- ▶ Genehmigung von Testinhalten durch Behörde und Vorlage der Testergebnisse

Bestehende IT-Regulierungen schaffen eine Basis für die effektive Umsetzung der DORA-Anforderungen

Auf Basis eines von unseren Experten durchgeführten umfassenden Abgleichs von DORA mit bestehenden Regularien, ist eine hohe Übereinstimmung erkennbar. Dennoch: Es existieren **wesentliche erweiterte und auch neue Anforderungen**, welche die vorhandenen europäischen und nationalen Vorgaben konkretisieren, verschärfen oder gänzlich ersetzen.

Abgleich DORA vs. MaRisk/BAIT (Auszug)

DORA - Anforderungen auf Einzelebene	MaRisk / BAIT	=	Wesentliche neue Anforderungen und Anpassungsbedarf sowie Auswirkung	
Artikel	DORA - Anforderungen	MaRisk/BAIT Referenz	Wesentliche Neuerung	Impact
Kap III Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle				
Artikel 17	Finanzunternehmen müssen angemessene Verfahren und Prozesse zur Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen einrichten und anwenden, einschließlich Frühwarnindikatoren, Kategorisierung und Klassifizierung, Zuweisung von Funktionen und Zuständigkeiten sowie Pläne für die Kommunikation und Reaktionsmaßnahmen.	BAIT Tz 3.10 Inforiskmgmt. BAIT Tz 4.7 - 4.10 ISMS BAIT Tz 5.3; 5.5 OplInfoSec BAIT Tz 8.6 IT-Betrieb MaRisk AT 7.2.4 Tech.-org. Ausstattung	- Einsatz von Frühwarnindikatoren zur Erkennung, Behandlung und Meldung von Vorfällen - Zuweisung von Funktionen und Zuständigkeiten für alle Arten von IKT-bezogenen Vorfällen - Erstellung von Kommunikationsplänen für Personal, externe Interessenträger, Medien, Kunden und andere Finanzunternehmen - Einführung von Prozessen zur Information an die Geschäftsleitung bei schwerwiegenden Vorfällen mit Erläuterung der Auswirkungen, Maßnahmen und zusätzlichen Kontrollen - Definition von Reaktionsmaßnahmen zur Minderung der Auswirkungen von IKT-Vorfällen und Sicherstellung der zeitnahen Verfügbarkeit und Sicherheit der Dienste	High
Artikel 18	Finanzunternehmen klassifizieren IKT-	BAIT Tz 4.7 ISMS	- Erweiterung der Analyse von IKT-bezogenen Vorfällen, um die Anzahl betroffener Kunden,	

Abb.: Abgleich DORA Anforderungen und MaRisk/BAIT

Mit der **BAIT-Novelle 2021** wurden neue Anforderungen im Bereich des Informationssicherheitsmanagements auf Basis der *EBA-Guidelines on ICT and Security Risk Management* eingeführt, die bereits viele Elemente von DORA aufgreifen. Unter anderem wurden in den Vorgaben zur „Operativen Informationssicherheit“ bereits Anforderungen im Bereich der Cyber Security definiert.

Aufbauend auf einem umfassenden Abgleich auf Ebene der einzelnen Anforderungen aus DORA, mit den bestehenden Vorgaben aus MaRisk und BAIT, ergeben sich einzelne Überschneidungen sowie Neuerungen. **Die konkreten Neuerungen, wie auch eine Einschätzung der Umsetzungsauswirkungen, haben wir analysiert und aufbereitet.**

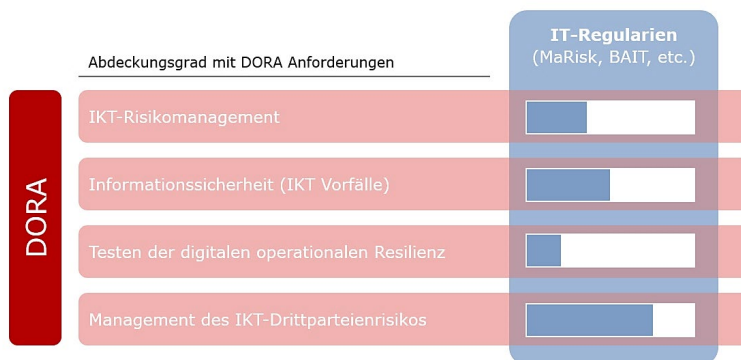







Abb.: Abdeckungsgrad DORA vs. IT-Regulation (MaRisk, BAIT)

Unsere Services – Ihr Nutzen

Für eine effektive Umsetzung der DORA-Vorgaben haben wir **effiziente und ressourcenschonende Vorgehensweisen** entwickelt. Diese berücksichtigen Best-Practices aus der **prüfungssicheren Umsetzung** von IT-Compliance Lösungen sowie die individuellen Rahmenbedingungen der Organisation gleichermaßen.

Mit unseren **DORA Services** unterstützen wir Finanzinstitute und IT-Dienstleister in der **fokussierten Analyse** bis hin zur **Umsetzung von maßgeschneiderten Lösungen und kompetenter Beratung** in allen Schwerpunktthemen der IT-Organisation.

Service	Umfang	
Gap-Analyse (moderiert)	<ul style="list-style-type: none"> Prüfung des Umsetzungsstandes der DORA-Anforderungen Moderierte Workshops zu den Bereichen der IT-Compliance Erarbeitung der IST-Situation und eines Zielbildes (Soll) Aufzeigen von Handlungsbedarf und konkreter Umsetzungsplanung 	
Webinare / Training	<ul style="list-style-type: none"> Transparenz über Schwerpunkte der DORA-Anforderungen Abgleich mit IT-Compliance Vorgaben Praktische Handlungshinweise und Prüfungserfahrungen Adressatengerechte Sensibilisierungsschulungen 	
IKT-Risiko-management	<ul style="list-style-type: none"> Etablierung eines IKT-Risikomanagements und dessen Verzahnung mit bestehenden Verfahren (u.a. OpRisk) Aufnahme und Bewertung des Risiko-Portfolios Erstellung von Risikoberichten Awareness-Training für Mitarbeiter und (Senior-)Management 	
Cyber-Security	<ul style="list-style-type: none"> Konzeption und Etablierung von IT-Asset-Management-Lösungen (CMDB) Prüfung und Optimierung von Verfahren zur Cyber-Security Etablierung eines Cyber-Security-Vorfallmanagements inkl. Reaktionsplänen 	
Outsourcing Management	<ul style="list-style-type: none"> Erstellung von Auslagerungsstrategien, Richtlinien und Verfahren zum Auslagerungsmanagement Konzeption und Durchführung von Risiko- und Vertragsanalysen, laufendes Auslagerungscontrolling, Exit-Strategien Regulatorische Begleitung und Absicherung von Auslagerungsvorhaben (u.a. Cloud Outsourcing) Unterstützung von IT-Dienstleistern zur regulatorisch-konformen Ausgestaltung von IT-Services 	

DORA Gap-Analyse – schnell und zuverlässig den Reifegrad der IT-Organisation ermitteln

Um **schnell und zuverlässig** einen Überblick über den Reifegrad der eigenen IT-Organisation zu erhalten und **konkreten Handlungsbedarf** zur Umsetzung der DORA-Anforderungen zu ermitteln, unterstützen wir zielgerichtet mit einem **praxiserprobten DORA Toolset**:

A	<p>Aufbau</p> <ul style="list-style-type: none"> Mehr als 400 Prüfungsfragen zu allen relevanten Themenbereichen (von IT-Strategie bis Security Testing) Erkenntnisse aus externen Prüfungen und laufenden Aufsichtsgesprächen Quantitativer und qualitativer Ansatz 	<p>4. Liegen für die "operative Informationssicherheit" in der schriftlich fixierten Ordnung die folgenden Dokumente vor?*</p> <table border="1"> <thead> <tr> <th></th> <th>Vollständig</th> <th>Eher mehr</th> <th>Eher weniger</th> <th>Gar nicht</th> </tr> </thead> <tbody> <tr> <td>Richtlinie für operative Informationssicherheit</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Standards für operative Informationssicherheit</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Vollständig	Eher mehr	Eher weniger	Gar nicht	Richtlinie für operative Informationssicherheit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Standards für operative Informationssicherheit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
	Vollständig	Eher mehr	Eher weniger	Gar nicht																							
Richtlinie für operative Informationssicherheit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																							
Standards für operative Informationssicherheit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																							
B	<p>Durchführung</p> <ul style="list-style-type: none"> Modulares Assessment, um den Erfüllungsstand effektiv zu bewerten und Lücken aufzudecken Fokussierte Einbindung der betroffenen Bereiche (u.a. IT-Governance, IT-Security, Auslagerungs-Management) Vorbereitete Checkliste für zielgerichtete Interviews und Workshops erleichtern die Analyse 	<table border="1"> <thead> <tr> <th></th> <th>Vollständig</th> <th>Eher mehr</th> <th>Eher weniger</th> <th>Gar nicht</th> </tr> </thead> <tbody> <tr> <td>Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte)</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Sichere Konfiguration von IT-Systemen (Härtung)</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Vollständig	Eher mehr	Eher weniger	Gar nicht	Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sichere Konfiguration von IT-Systemen (Härtung)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Vollständig	Eher mehr	Eher weniger	Gar nicht																							
Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																							
Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																							
Sichere Konfiguration von IT-Systemen (Härtung)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																							
Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																							
C	<p>Auswertung</p> <ul style="list-style-type: none"> Einwertung der Antworten anhand von Best-Practices und Prüfungsstandards Auswertung je Themengebiet (Detailreport) und gesamthaft (Management Report) Praxisnahe Vorschläge für konkrete Handlungsmaßnahmen je Themengebiet als Basis für die individuelle Umsetzungsplanung 																										

Zur Unterstützung des Quick-Checks und der Analyse haben wir Webinare zu verschiedenen Themenstellungen, die einen tieferen Einblick in die neuen Anforderungen bieten.



Webinar: DORA - Neuer EU-Rahmen für Cyber-Resilienz in Finanzunternehmen



Blog: Neue regulatorische Vorgaben rund um DORA



Auszug Präsentation VAB: Informationssicherheit im Rahmen des IKT-Risikomanagements



Unsere Expertise in der IT- Compliance

Severn verfügt über **langjährige Erfahrungen** und **fundierte fachliche wie auch methodische Kenntnisse** in der Etablierung von IT-Management Lösungen. Dabei kombinieren wir unsere Erfahrung und **Kenntnisse der Prüfungspraxis der Aufsicht** mit **praxiserprobten Verfahren** zur Umsetzung des individuellen Handlungsbedarfs.

Wir verstehen uns als Partner der IT und konnten dies für namhafte Kunden in zahlreichen erfolgreich durchgeführten Projekten bereits unter Beweis stellen

Referenzprojekte (Auszug):

- ▶ **Internationales Finanzunternehmen:** Aufbau eines IT Compliance Frameworks und Umsetzung der BAIT/MaRisk sowie EBA-Vorgaben, Konzeption von Zielbildern bis Transition in die Organisation (u.a. Schulung von mehr als 200 Mitarbeitern). Durchführung einer „Audit-Simulation“ zur Verprobung von Wirksamkeit und Angemessenheit.
- ▶ **Depotbank:** Nachhaltige Behebung von Feststellungen der EZB in den Bereichen: IT-Risk-Management, Identity & Access Management, Business Continuity Management, Outsourcing, Application Development / EUC, Berichterstattung an Aufsicht
- ▶ **Bank:** Behebung von Feststellungen aus IT-Sonderprüfung, Entwicklung von Zielbildern und Umsetzungsmaßnahmen in allen wesentlichen IT-Funktionen, Kommunikation mit Aufsichtsbehörden und Prüfern, Change- und Roll-out Management
- ▶ **Internationaler Börsenkonzern:** Durchführung von „Audit-Simulationen“ und Prüfungsvorbereitung. Aufbau eines neuen IT Compliance Frameworks und Umsetzung der BAIT/MaRisk sowie EBA-Vorgaben nach erfolgter Sonderprüfung, Konzeption von Zielbildern und Entwicklung neuer agiler technologischer Plattformen (OpenShift).
- ▶ **Förderinstitut:** Behebung von Feststellungen im Identity & Access Management (IAM), Umsetzung von prozessualen und technischen Maßnahmen im Berechtigungsmanagement, Anbindung von Applikationen an eine zentrale IAM-Lösung
- ▶ **Landesbank:** Steuerung und Umsetzung eines Gesamtprogrammes zur Behebung von Feststellungen in der IT-Compliance, insbesondere IT-Governance, IT-Strategie, IT-Risikomanagement, Auslagerungsmanagement und IAM
- ▶ **Versicherungskonzern:** Begleitung einer IT-Sonderprüfung, Beratung und Qualitätssicherung, Unterstützung in der VAIT-Umsetzung (u.a. operative IT-Sicherheit, IDV, Ausgliederungsmanagement)

Zu unseren Kunden zählen u.a.:



Ihr Partner

Next Generation Consulting für Finanzunternehmen

Severn Consultancy ist eine auf den nationalen und internationalen Finanzmarkt spezialisierte Unternehmensberatung. Unsere besondere Expertise liegt in der effektiven Realisierung erfolgskritischer Veränderungsprozesse in der Marktfolge – dort sind wir besser als viele andere.

Exzellente Beratung und sofort wirksame Lösungen für unsere Mandanten – mit diesem Anspruch wurde Severn 1987 gegründet. Kompetente Fach- und Managementberatung gepaart mit effektivem Projektmanagement sind die Säulen des „Severn ways to get it done“.



In mehr als 20 Jahren Beratungspraxis haben wir eine Vielzahl renommierter Unternehmen bei der effizienten Durchführung ihrer Projekte und der Optimierung unternehmensinterner Prozesse unterstützt. Unsere Mandanten schätzen unsere innovativen Beratungskonzepte, das methodische Know-how sowie unsere fundierten Markt- und Branchenkenntnisse.

Wir verstehen Ihre Anforderungen, kennen die Themen und unterstützen Sie schnell und flexibel mit wirkungsvollen Lösungen. Wir liefern zuverlässig konkrete Ergebnisse, die Ihnen messbaren Erfolg bringen. Nehmen Sie uns beim Wort und erleben Sie Next Generation Consulting.

Ansprechpartner:

Severn Consultancy GmbH
Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
T +49 (0)69 / 950 900-0
info@severn.de
www.Severn.de



Norman Nehls
Partner



Marco Gabor
Projektmanager

© 2023 Severn Consultancy GmbH

Disclaimer

Die Inhalte der folgenden Seiten wurden von Severn mit größter Sorgfalt angefertigt. Severn übernimmt jedoch keinerlei Gewähr für die Aktualität, Korrektheit und Vollständigkeit der bereitgestellten Informationen. Haftungsansprüche gegenüber Severn, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern vonseiten Severn kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt. Severn behält sich ausdrücklich vor, Teile der Seiten ohne gesonderte Ankündigung zu verändern, zu ergänzen und/oder zu löschen. Alle Rechte vorbehalten. Die Reproduktion oder Modifikation ganz oder teilweise ohne schriftliche Genehmigung von Severn ist untersagt