

# SEEBURGER

>< Connect >> Automate >>> Innovate

 Webcast-Serie | Meet the Expert

## EU-NIS 2 und das deutsche NIS2UmsuCG steht vor der Tür!

Wie können Sie als Kunde  
SEEBURGER als Ihren  
Dienstleister einfach prüfen?





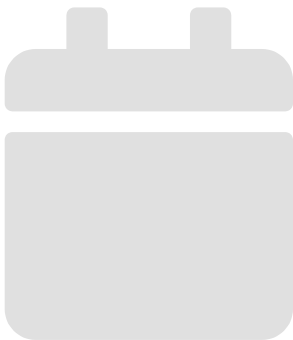
# Disclaimer

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. SEEBURGER erbringt mit dieser Veröffentlichung keine professionelle Dienstleistung, insbesondere keine rechtliche oder steuerliche Beratungsleistung. Diese Veröffentlichung ist nicht geeignet, um unternehmerische Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater (z. B. Rechtsanwalt und/oder Steuerberater) in Bezug auf den Einzelfall beraten lassen. Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht.

SEEBURGER haftet nicht oder ist nicht verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Informationen aus der Präsentation entstehen.

# Agenda

- 01** | EU-NIS 2 & EU-RCE steht vor der Tür
- 02** | Gesetze in EU-Mitgliedstaaten  
(Beispiel NIS2UmsuCG)
- 03** | Informationssicherheit bei SEEBURGER
- 04** | Überprüfen Sie Ihre Lieferkette
- 05** | Nächste Schritte bei SEEBURGER



**01**

EU-NIS 2 & EU-RCE  
steht vor der Tür



# Vergleich von EU-NIS2, EU-RCE und EU-DORA

	NIS 2	RCE	DORA
Schwerpunkt	Cyber-Sicherheit	Widerstandsfähigkeit kritischer Systeme	Cybersicherheit und Widerstandsfähigkeit
Umfang	Die Definitionen der Sektoren umfassen bis zu 50 % der Unternehmen	Kritische Systeme (Ersatz für KritisV bzw. BSIG §8.1a)	Finanzindustrie (ersetzt BAIT, VAIT und ZAIT....)
Anforderungen	Governance (§ 20), Cyber-Hygiene, Reaktion auf Vorfälle, Management der Geschäftskontinuität, Sicherheit der Lieferkette (§21), Meldekette an das BSI (§23)	Physische Sicherheit, Business Continuity Management und Disaster Recovery im Detail	Widerstandsfähigkeit des Betriebs und der IT, Incident Management, Business Continuity Management & Disaster Recovery im Detail
Relevanz für SEEBURGER	Direkt als Anbieter von Cloud- und Managed Services (CSP & MSP)	Nein, da wir keine kritischen Systeme betreiben (oder betreiben werden)	Indirekt als normaler ICT-Dienstleister §30.2 aber nicht unter §30.3 (wichtig oder kritisch)
Start	18.10.2024	18.10.2024	17.01.2025

# Neue Compliance-Anforderungen 2024 – EU-NIS 2

- NIS 2 = Richtlinie über die Sicherheit von Netz- und Informationssystemen  
*"Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit 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)"*
- EU-NIS 2 ist keine Verordnung wie EU-GDPR, sondern eine EU-Richtlinie. Sie muss eigentlich bis Oktober 2024 in den jeweiligen EU-Mitgliedsstaaten Gesetz werden (oder wird indirekt aktiv)
- Unterscheidung zwischen "kritisch" (bisher KRITIS §8a / Deutschland), "sehr wichtig" und "wichtig"
- Der *EU NIS 2 Implementation Act* (ETA 24.10.2024) regelt die Details



Governance  
Artikel 20



Risikomanagement und  
Maßnahmen  
Artikel 21



Berichterstattung  
Artikel 23



Europäische Cyber-  
Zertifizierungen  
Artikel 24

# Neue Compliance-Anforderungen 2024 - Unternehmen im Geltungsbereich

## Sektor 1

- Energie
- Transport
- Banken
- Finanzmärkte
- Anbieter im Gesundheitswesen
- Trinkwasser
- Abwässer
- Digitale Infrastruktur
- **IKT-Dienstleistungsmanagement**
  - Anbieter von Cloud-Diensten **SEEBURGER**
  - Anbieter Managed Services Dienste
- Anbieter von Managed Security Services
- (Öffentliche Verwaltung)
- Weltraum

## Sektor 2

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemikalien
- Lebensmittel
- Herstellung
- Digitale Dienste
- Forschung

## Größe

EU-NIS 2 verwendet einheitliche Kriterien (2003/361/EG) zur Identifizierung der Betreiber auf der Grundlage der Unternehmensgröße, um die unterschiedlichen Schwellenwerte in der EU zu harmonisieren:

- **Großunternehmen:  $\geq 250$  Beschäftigte,  $> 50$  Mio. EUR Umsatz,  $> 43$  Mio. EUR Bilanz** **SEEBURGER**
- **Mittlere Unternehmen:  $< 250$  Beschäftigte,  $\leq 50$  Mio. EUR Umsatz,  $\leq 43$  Mio. EUR Bilanz**

# Neue Compliance-Anforderungen 2024 – Ein Kick an Cybersicherheitsanfragen wie bei EU-GDPR 2018



## Bisherige Regulierung

### 1. Deutschland

1. Legacy KRITIS §8a : 3.000 Unternehmen
2. Legacy KRITIS §8c : weitere 3.000 Unternehmen ?
3. Finanzen: BAFIN (BAIT, ZAIT & VAIT)

### 2. Andere EU-Mitgliedstaaten hatten oft vergleichbare Regelungen (außer im Finanzbereich)

## Ab 18.10.2024

1. In Deutschland sind ~30.000 Unternehmen betroffen
2. In anderen Teilen der EU kommen weitere ~30.000 Unternehmen hinzu

**Die Zahl der regulierten Unternehmen steigt wegen der EU-NIS 2 massiv**

**Wir erwarten viele Anfragen zur Cybersicherheit (ähnlich wie bei der GDPR 2018)**



# Digital Operational Resilience Act (DORA) EU-Verordnung 2022/2554



DORA ist im Grunde wie NIS 2 auf Steroiden für Unternehmen auf den Finanzmärkten

DORA ist seit dem 16.01.2023 in Kraft und die Umsetzungsfrist von zwei Jahren endet am 17.01.2025

DORA beauftragt die Europäischen Aufsichtsbehörden (ESAs = EBA, EIOPA und ESMA), technische Standards im Rahmen von Rechtsakten zu definieren

SEEBURGER ist als IKT-Anbieter indirekt betroffen (Management des IKT-Drittparteirisikos Artikel 28 bis 44)

Wie andere ICT-Anbieter ist SEEBURGER praktisch doppelt reguliert

SEEBURGER handelt als "normaler" IKT-Anbieter gemäß Artikel 30.2

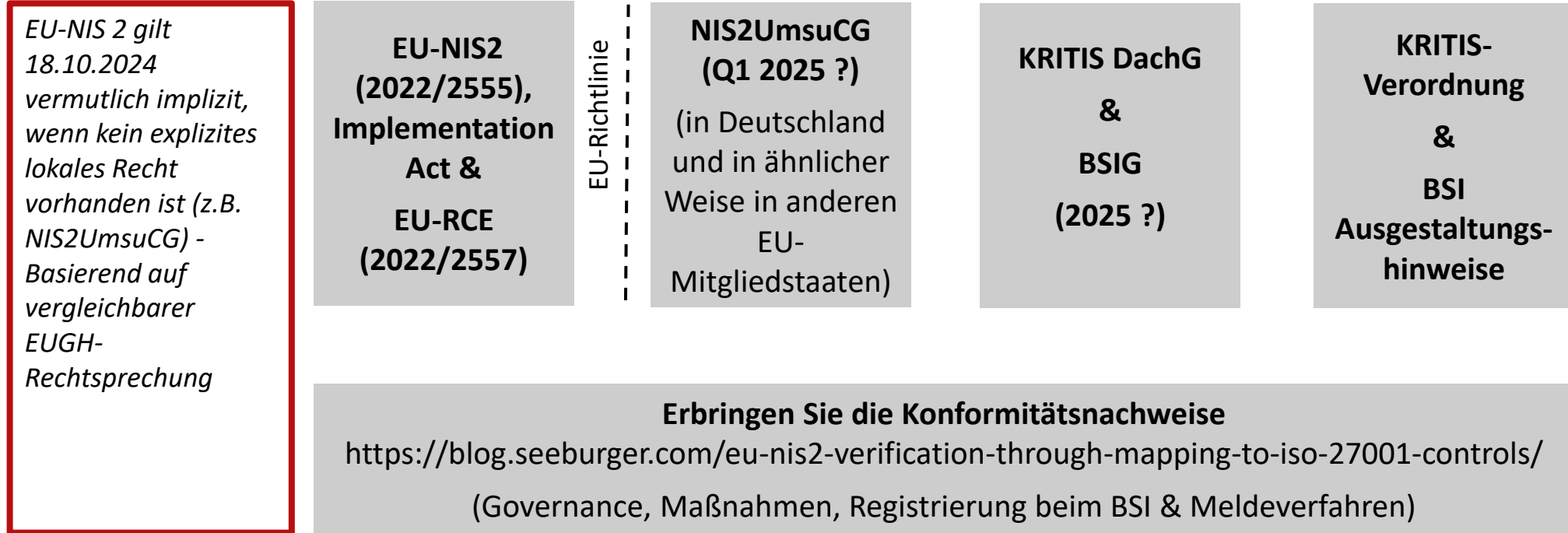
# 02

Gesetze in EU-  
Mitgliedstaaten  
(Beispiel  
NIS2UmsuCG)



# EU-NIS 2 Gesetz in Deutschland zur EU-NIS 2 und das entsprechende Ausführungsgesetz

## Voraussichtliche Abfolge der Aktualisierungen



## Unterstützung des Prozesses

# Der SEEBURGER-Ansatz

## Vorbereitung mit Zertifizierungen 2024 auf EU-NIS

- 1) Abschluss der Umstellung auf ISO 27001:2022
- 2) Prüfen Sie, ob Ihr ISO 27001:2022 Geltungsbereich ausreicht
- 3) Prüfen Sie den NIS 2 EU Implementation Act (ETA 24.10.2024)
- 4) Compliance-Nachweise: ISO 27001 → EU-NIS 2 Artikel 21 und Implementation Act
- 5) Wirksamkeitsnachweise hinzufügen, falls vorhanden
  - ISAE 3402 SOC 1 Typ 2
  - TISAX (nur alle 3 Jahre)
  - BSI C5....
- 6) Lokale Cyber-Agentur (z. B. BSI in Deutschland)
  - Registrierung bei der Cyber-Agentur
  - Verfahren zur Meldung von Sicherheitsvorfällen
- 7) Erwägen Sie
  - Weitere Vorgaben aus dem lokalen Recht (z.B. NIS2UmsuCG)
  - Umfassendes Lieferantenmanagement

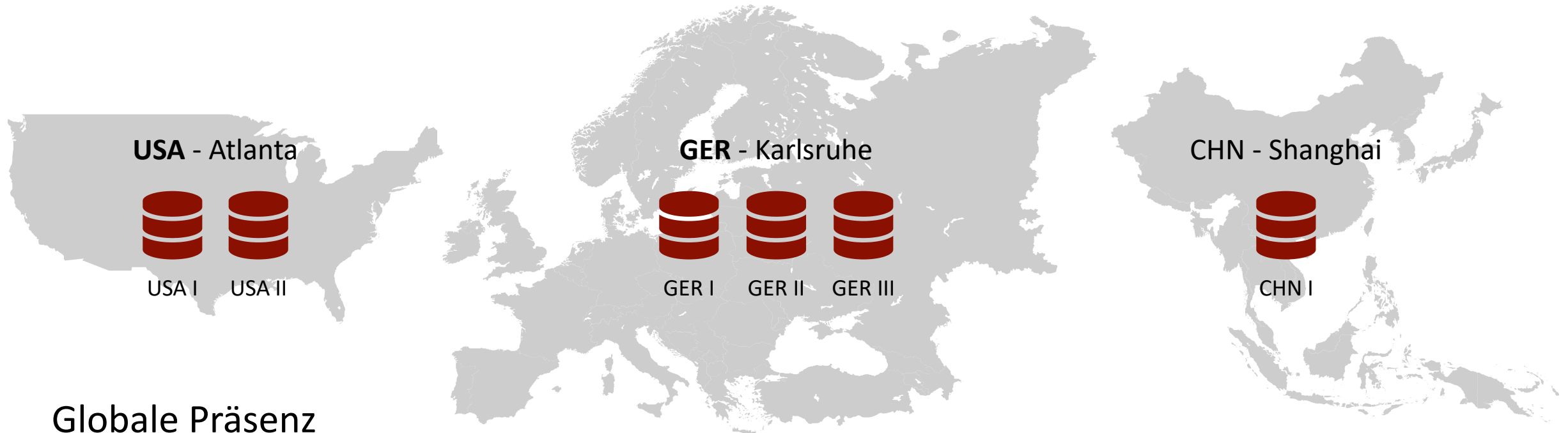


03

Informations-  
sicherheit  
bei SEEBURGER



# SEEBURGER Rechenzentren - Technische und betriebliche Maßnahmen (TOMs) für die Cloud



## Globale Präsenz

- + ISO Geltungsbereich  
"SEEBURGER Cloud Services EDI / B2B, GTS und iPaaS Operations mit den Prozesskomponenten Go-Live, Incident Management, Event Management & Monitoring, Change Management sowie den unterstützenden IT-Prozessen"
- + Tier 3+ Rechenzentren in Deutschland, China und den USA
- + Internationale Datenschutzabkommen (IGDTA)
- + ISO/IEC 27001-Zertifizierung, jährlich seit 2012
  - + Die Migration von ISO/IEC 27001:2017 auf 27001:2022 erfolgt von SEEBURGER-Seite aus
  - + Aufgrund der 3-Jahres-Zertifizierung wird unser ISO 27001-Zertifikat dies Q3 2025 vollständig widerspiegeln.
- + ISAE 3402 SOC 1 Typ 2, jährlich seit 2017
- + TISAX-Zertifizierung
  - + Wirksamkeitsprüfung und Bescheinigung von ISO 27001
  - + seit 2020 in einem 3-Jahres-Zyklus

# SEEBURGER Informationssicherheits-Zertifizierungen 2024 auf einen Blick

## ISO 27001

- + Nachweis, dass die Organisation ein wirksames Informationssicherheitsmanagementsystem (ISMS) eingeführt hat
- + International anerkannter Standard
- + De-facto-Standard, den alle unsere Kunden fordern
- + Kontrollmechanismen aus der ISO 27002
- + Seit 2012 jährlich durch eine Wirtschaftsprüfung (KPMG) verifiziert

## ISAE 3402 SOC 1 Typ 2

- + Nachweis, daß die Kontrollen tatsächlich durchgeführt werden
- + Prüfung auf der Grundlage von rückwirkenden Stichproben im Berichtszeitraum (12 Monate)
- + Liefert sehr spezifische Informationen über die Qualität und Wirksamkeit der durchgeführten Kontrollen
- + Detaillierter Auditbericht, der Kunden zur Verfügung gestellt wird
- + Jährliche Überprüfung durch die Wirtschaftsprüfungsgesellschaft (KPMG) seit 2017
- + Telemaxx hat inzwischen einen eigenen SOC 1-Bericht

## TISAX

- + Effektivitätskontrolle in der Automobilindustrie
- + Branchenspezifischer Nachweis der Informationssicherheit auf der Grundlage von ISO 27001 mit vordefiniertem Umfang
- + Klassifizierung nach Bewertungsstufen und Reifegraden
- + Seit 2020 alle 3 Jahre durch ein externes Audit (KPMG) verifiziert

# Betriebsformen



**Eigenbetrieb durch den Kunden**



**iPaaS**



**Managed Services Cloud**

Betriebsform	Eigenbetrieb durch den Kunden	iPaaS	Managed Services Cloud
Handelspartner-Management	Blue bar	Blue bar	Red bar
Änderungsmanagement	Blue bar	Blue bar	Red bar
Kartierung der Entwicklung	Blue bar	Blue bar	Red bar
Management von Zwischenfällen	Blue bar	Blue bar	Red bar
Erkennung von Zwischenfällen	Blue bar	Blue bar	Red bar
BIS-Freigabe-Management	Blue bar	Red bar	Red bar
Betrieb und Pflege der Datenbank	Blue bar	Red bar	Red bar
Betrieb und Wartung von OS	Blue bar	Red bar	Red bar
Netzwerk	Blue bar	Red bar	Red bar
Hardware und Infrastruktur	Blue bar	Red bar	Red bar
Unterstützung für On Premises	Red bar	Nicht erforderlich	Nicht erforderlich
Beratung	Red bar	Optional	Optional
BIS Entwicklung	Red bar	Red bar	Red bar

ISO 27001 (TISAX & ISAE 3402 SOC 1)

ISO 27001, TISAX & ISAE 3402 SOC 1

Prozesse für BIS Development, Support für On Premises und Consulting-Kunden sind eine Untermenge und folgen angepassten, aber im Prinzip ähnlichen Spezifikationen, sind aber nicht explizit Teil des Zertifizierungsumfangs.

- Kunde
- SEEBURGER



# ISO27001:2022 A.5 Management von Sicherheitsvorfällen

## Beispiel für Bedrohungsanalyse und PEN-Tests für Cloud-Kunden


- Auslöser für den Sicherheitsvorfallprozess

- Benachrichtigung/Vorfall
- Wichtige Erkenntnisse
  - PENTests
  - Schwachstellen-Scans
  - Prüfungen
- Wichtige CVEs

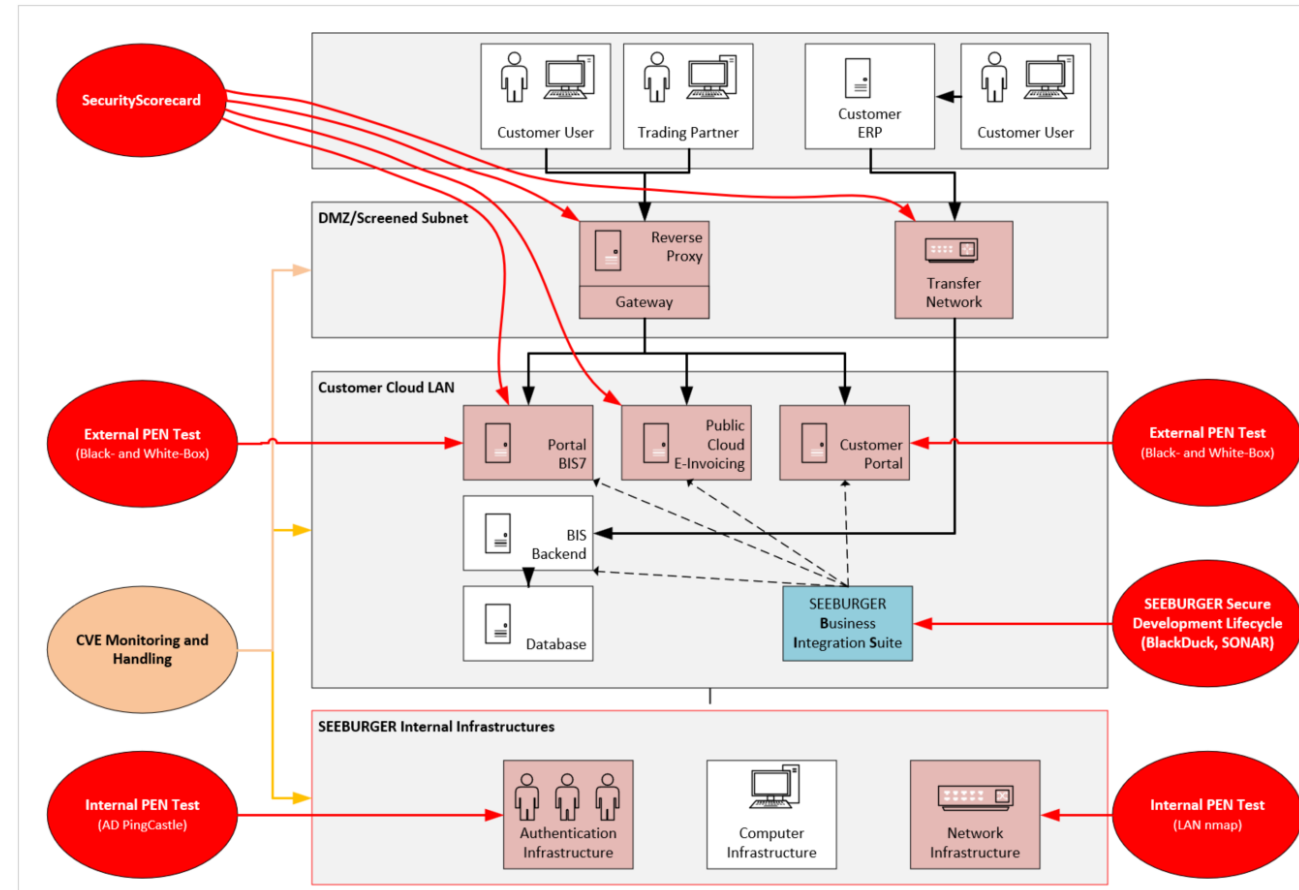
- Werkzeuge und Ressourcen

- Pink Castle
- KALI Linux
- NTFS-Berechtigungsreporter
- Sicherheits-Scorecard: 96 / 100 (23.09.2024)

 **SEEBURGER AG Security Rating**  
seeburger.com

 **A** 96 / 100

- CVE-Überwachung



# ISO27001:2022 A.5 Management von Sicherheitsvorfällen

## Kunden vor Ort Bedrohungsanalyse und PEN-Tests

- SEEBURGER unterstützt On Premises Kunden bei sicherheitsrelevanten Aspekten von SEEBURGER Software und Lösungen auf der Basis von Schwachstellenbehandlung und entsprechender Offenlegung
- Fehler können durch die Bereitstellung von Anleitungen, Patches, Hotfixes oder neuen Releases der Software behoben werden. Details sind in der Dokumentation und den Release Notes über den SEEBURGER Service Desk abrufbar.
- Bietet SEEBURGER im Rahmen der Softwarepflege dem Kunden einen Patch, Hotfix oder ein neues Release zur Fehlerbehebung an, so ist der Kunde verpflichtet, diesen auch anzunehmen und ist für die Installation verantwortlich

### PEN Tests kombiniert im Jahr 2024 (Stand 23.09.2024):

- Informationssicherheit
  - Geplante Tests: 7
  - Tests in Arbeit: 2
  - Durchgeführte Tests: 2
- Unternehmens-IT
  - Geplante Tests: 1
  - Laufende Tests: 1
  - Durchgeführte Tests: 0
- Cloud-IT
  - Geplante Tests: 5
  - Laufende Tests: 1
  - Durchgeführte Tests: 1
- Entwicklung
  - Geplante Tests: 2
  - Laufende Tests: 1
  - Durchgeführte Tests: 1
- **Zusammenfassung 2024 bis dahin**
  - **Insgesamt geplante Tests: 15**
  - **Laufende Tests: 5**
  - **Durchgeführte Tests: 4**

Sicherheits-Scorecard: 96 / 100

# ISO27001:2022 Anhang 5.29, 5.30 & 8.14 Management der Geschäftskontinuität

Es gibt BCP- und DR-Pläne für eine mögliche Unterbrechung bei der Erbringung von Dienstleistungen, Support und Consulting

SEEBURGER bereitet sich auf Notfälle, Krisen und Katastrophen auf Basis der ISO 27001 vor

Wir greifen auch auf bewährte Praktiken des BSI (Bundesamt für Informationssicherheit - IT Grundschutzkompendium 200-4) zurück, wobei wir uns auf aktuelle Cybersicherheitsszenarien konzentrieren

Cyber-Krisenmanagement [EDIT LINKS](#)

## Taskforce\_BCM\_RP\_Plans · English\_2024

[+ new document](#) or drag files here

All Documents

✓	Name	Modified	Version
	Supplemental_Procedures	... August 1, 2023	1.0
	1_ISO_27001_Policy_A5-29etal_BCM_2025_EN	... August 23	1.0
	2a_KS-Cyber-Crisis_Managementplan_2024	... August 15	17.0
	3a_KS_Team_Roles_2024	... August 23	20.0
	3b_KS_Role_Cards_2024	... August 15	9.0
	3c_KS_Communication_FAQ_Crisis_Management_plan_2024	... August 6	4.0
	3d_KS_Protocol_Template_2024	... August 6	8.0
	3e_KS_Simple_Protocol_Template_Meeting_2024	... August 6	8.0
	3f_KS_Vizualisation_Template_2024	... August 6	10.0
	4_BCM_Administration_Marketing_2024	... August 13	9.0
	4_BCM_AdministrationPayment-HR_2024	... August 13	10.0
	4_BCM_Cloud_IT_2024	... 4 days ago	8.0
	4_BCM_Consulting_2024	... August 9	12.0
	4_BCM_Development_2024	... August 13	11.0
	4_BCM_Sales_2024	... August 13	13.0
	4_BCM_SEEBURGER_Informatik_EOOD_BG_2024	... August 13	4.0
	4_BCM_SEEBURGER_US_2024	... August 13	5.0
	4_BCM_Support_2024	... August 13	9.0

# Drittanbieter zur Abschätzung der Informationssicherheit

## Plattformen zur Bewertung von Cyberrisiken (CRR)

- CRRs scannen von außen nach Schwachstellen und liefern eine allgemeine Bewertung
- SEEBURGER nutzt und pflegt:  
<http://securityscorecard.com/security-rating/seeburger.com>
- SEEBURGER kann nicht alle anderen ebenfalls pflegen, z.B.
  1. Bitsight
  2. Black Kite
  3. BlueVoyant
  4. ISS Corporate Solutions
  5. Locate Risk
  6. Panorays
  7. Prevalent
  8. Recorded Future
  9. Risk Recon
  10. UpGuard.....

## Risikomanagement-Plattformen (TPRM)

- TPRMs sind Meta-Plattformen zur Bewertung der bereitgestellten Informationen (Zertifizierungen usw.)
- TPRMs können CRR-Funktionalität enthalten
- SEEBURGER pflegt keine TPRMs, z.B.
  1. Aravo
  2. Archer
  3. Cybervadis
  4. Diligent TPM
  5. Exiger
  6. IBM OpenPages
  7. LogicGate
  8. MetricStream TPM
  9. Navex
  10. Onetrust TPM
  11. Prevalent
  12. ProcessUnity
  13. ServiceNow TPM
  14. Venminder.....

04

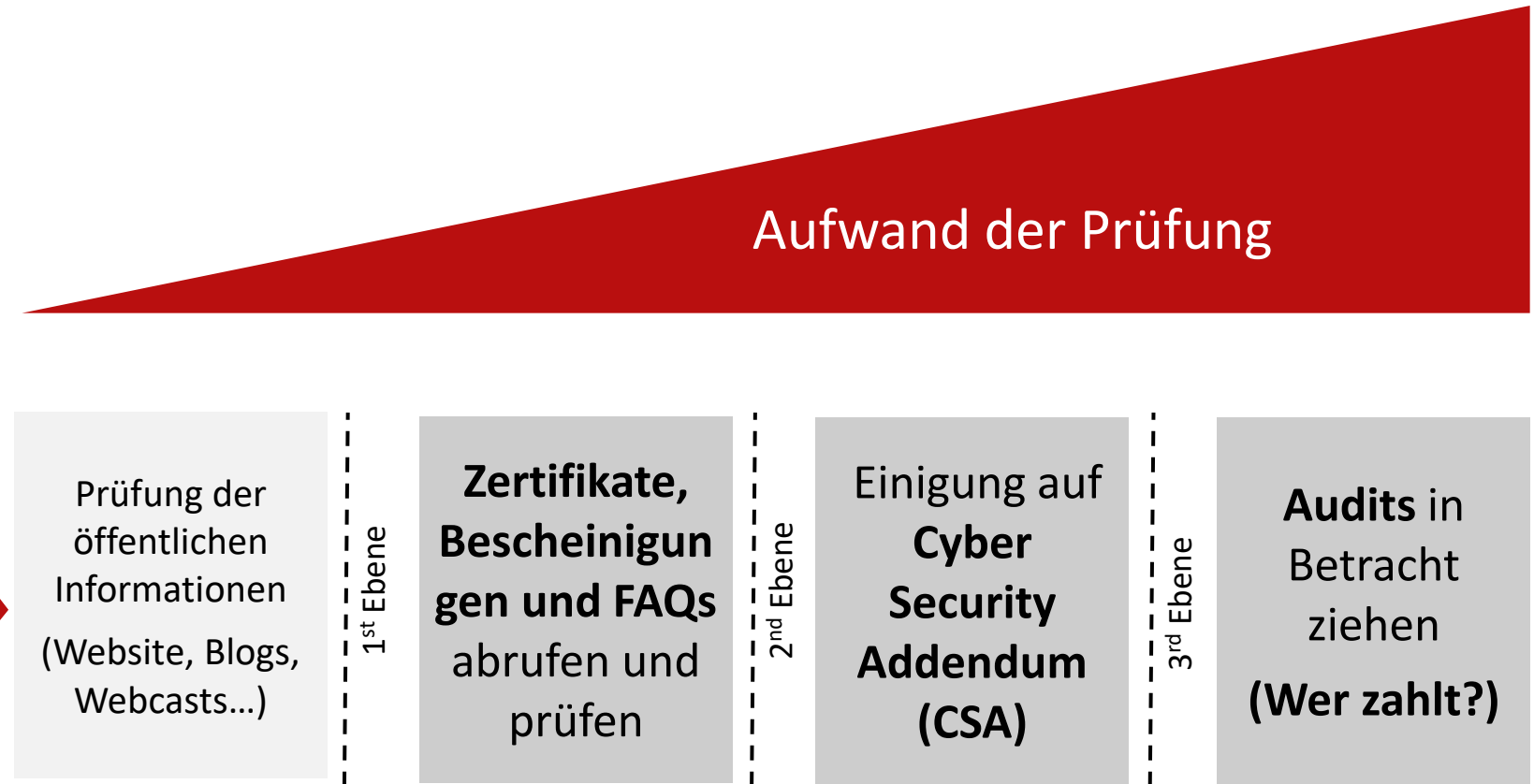
Überprüfen Sie Ihre  
Lieferkette



# Informationssicherheit & EU-NIS 2

## Prüfen Sie Lieferanten mit einem strukturierten Beurteilungsprozess

1. Zentrales Lieferantenregister
2. Interne Ansprechpartner
3. Anwendungsfall und Design Ihrer Lösung
4. Auftragswert hinzufügen
5. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Kritikalität für die Lieferkette hinzufügen
6. Prioritäten für Lieferanten setzen
7. **Anbieter prüfen**
8. Dokumentieren Sie die Abweichungen in Ihrem Risikomanagement



# Informationssicherheit & EU-NIS 2

## EU NIS 2 Implementation Act

Das EU-NIS 2 Implementation Act NIS 2 regelt die Details der Artikel 20 & 21 und definiert signifikante Incidents des Artikels 23

ISO 27001:2022 Zuordnungen sind verfügbar:

- <https://blog.seeburger.com/eu-nis2-verification-through-mapping-to-iso-27001-controls/>
- <https://www.openkritis.de/massnahmen/implementing-acts-it-nis2-mapping.html>

### Entwurf

- [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en)  
→ Entwurf einer Durchführungsverordnung und des Anhangs - Ares(2024)4640447
- Tritt voraussichtlich am 24.10.2024 in Kraft

**Der NIS 2 Implementation Act 5.1.4. wird zu Cybersicherheitszusatzvereinbarungen (CSAs) führen, die den DSGVO AVVs §28 (Datenschutzvereinbarungen) von 2018 ähneln**

- IKT-Lieferanten haben ihre eigenen Cybersicherheitsstandards
- Vernünftiger Ansatz, den IKT-Lieferanten akzeptieren und auch an ihre Lieferanten weiterreichen können
- Reduzieren Sie den Aufwand für sich und IKT-Lieferanten durch relevante Zertifizierungen
- Ziel: Angemessene Antwortquoten und rasche Antworten

# EU-NIS 2 Artikel 21.2 (d) & 21.3 Lieferantenmanagement – EU IT Implementation Act Article 5.1.4

## Cyber Security Addendum

### EU IT Implementation Act 5.1.4.

Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities **shall ensure that their contracts with the suppliers and service providers specify**, where appropriate through service level agreements, specify the following, **where appropriate**:

- (a) cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;
- (b) requirements regarding skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;
- (c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2.;
- (d) an obligation on suppliers and service providers to notify, **without undue delay**, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;
- (e) provisions on repair times;
- (f) **the right to audit or right to receive audit reports**;
- (g) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;
- (h) requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);
- (i) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.....



Brussels, XXX  
[...] (2024) XXX draft

ANNEX

ANNEX

to the

Commission Implementing Regulation

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers



05

Nächste Schritte zur  
Überprüfung von  
SEEBURGER



# Informationssicherheit & EU-NIS 2

## Individuelle Kundenanfragen

**SEEBURGER wird Anfragen hauptsächlich nach Eingangsdatum und Komplexität der Anfrage priorisieren**

**SEEBURGER hält nicht für geeignet**

1. Große Excel-Tabellen im Freestyle
2. Portalfragebögen, da diese aufgrund des Mangels an juristischen Beweisen ein hohes Risiko darstellen
3. TPRM-Portale
  - <https://www.processunity.com/> usw.
  - Oft außerhalb von EU DSGVO und EU AI Act
  - TPRM verlangen, dass SEEBURGER die jeweiligen TPRM-AGBs akzeptiert. In der Regel nutzen sie unser geistiges Eigentum und unsere Inhalte, um ihre eigene KI zu trainieren.
  - TPRM verlangen von SEEBURGER jährliche Zahlung und Wartung

**SEEBURGER Informationssicherheit liefert nach dem SEEBURGER-Standard und CSA**

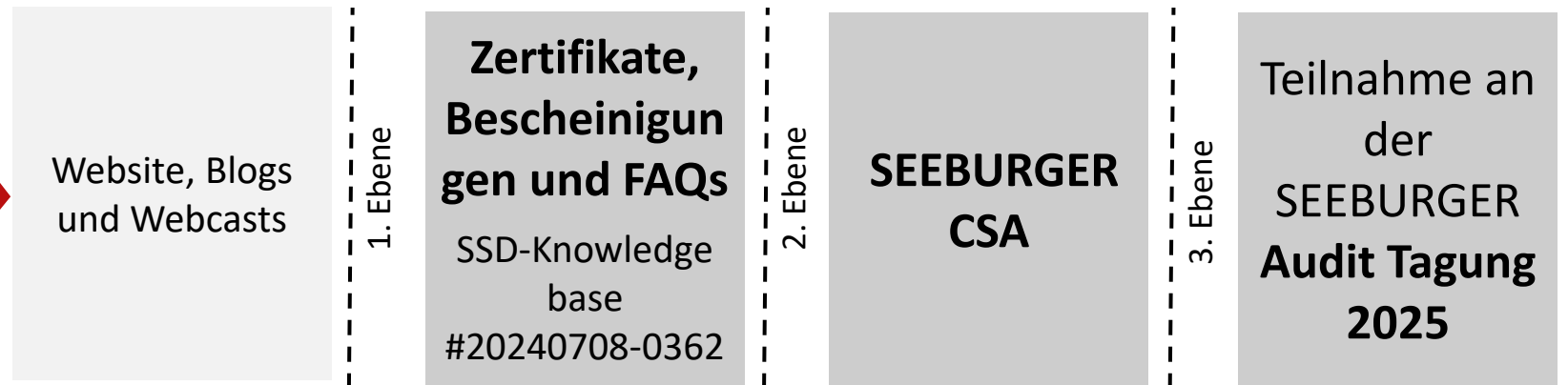
**SEEBURGER hält nicht für geeignet**

1. Externe Verträge zur Cybersicherheit mit
  - Unklare TOMs
  - Zusätzliche Garantien wie
    - "Unverzüglich" anstelle von "ohne unnötige Verzögerung"
    - SLAs....
  - Die Beweislast liegt bei SEEBURGER
  - Verschärfte Haftung
  - Prüfungsrechte ohne Begrenzung und Bezahlung
  - Erforderliche Nachweise über den SEEBURGER Standard hinaus
2. Kosten für externen Rechtsbeistand oder Anforderungen für Verhandlungen

**Stattdessen möchten wir uns auf die eigentliche Informationssicherheit konzentrieren und Zertifizierungen erweitern, um die Sicherheit unserer gesamten installierten Basis zu erhöhen.**

# Prüfen Sie SEEBURGER in Übereinstimmung mit Ihrem strukturierten Beurteilungsansatz

1. Finden Sie Ihre eigenen internen Ansprechpartner
2. Dokumentieren Sie Use Case und Einrichtung Ihrer SEEBURGER-Lösung
3. Auftragswert hinzufügen
4. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Kritikalität für die Lieferkette hinzufügen
5. Priorisieren Sie Ihre Lieferanten
6. **SEEBURGER prüfen**
7. Dokumentieren Sie die Abweichungen in Ihrem Risiko Management



Wenden Sie sich an Ihren SEEBURGER-Ansprechpartner im Vertrieb für unser Cyber Security Addendum (EU NIS 2 Implementation Act Artikel 5.1.4)

SEEBURGER liefert im Sinne des SEEBURGER CSA, auch wenn der Kunde nicht unterschrieben hat. Dies ist unser Standard auf Basis ISO 27001 und NIS 2

**Nachweis der nötigen Sorgfalt**



## 2024 SEEBURGER AG. All rights reserved.

The information in this document is proprietary to SEEBURGER. Neither any part of this document, nor the whole of it may be reproduced, copied, or transmitted in any form or purpose without the express prior written permission of SEEBURGER AG. Please note that this document is subject to change and may be changed by SEEBURGER at any time without notice. SEEBURGER's Software product, the ones of its business partners may contain software components from third parties.

As far as reference to other brands is concerned, we refer to the following:

SAP®, SAP® R/3®, SAP NetWeaver®, SAP Cloud Platform & Cloud Platform Integrator®, SAP Archive Link®, SAP S/4HANA®, SAP® GLOBAL TRADE Service® (SAP GTS), SAP Fiori®, ABAP™ and SAP ARIBA® are registered trade marks of the SAP SE or the SAP Deutschland SE & Co. KG (Germany). Microsoft, Windows, Windows Phone, Excel, Outlook, PowerPoint, Silverlight, and Visual Studio are registered trademarks of Microsoft Corporation in the United States and other countries. Linux is a registered trade mark of Linus Torvalds in the United States and other countries. UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group. Adobe, the Adobe logo, Acrobat, Flash, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and / or other countries. HTML, ML, XHTML, and W3C are trademarks, registered trademarks, or claimed as generic terms by the Massachusetts Institute of Technology (MIT), European Research Consortium for Informatics and Mathematics (ERCIM), or Keio University. Oracle and Java are registered trademarks of Oracle and its affiliates.

All other company and software names mentioned are registered trademarks or unregistered trademarks of their respective companies and are, as such, subject to the statutory provisions and legal regulations. 4invoice®, iMartOne®, SEEBURGER®, SEEBURGER Business-Integration Server®, SEEBURGER Logistic Solution Professional®, SEEBURGER Web Supplier Hub®, WinELKE®, SEEBURGER File Exchange®, SEEBURGER Link®, SMART E-Invoice® and other products or services of SEEBURGER which appear in this document as well as the according logos are marks or registered marks of the SEEBURGER AG in Germany and of other countries worldwide. All other products and services names are marks of the mentioned companies.

All contents of the present document are noncommittal and have a mere information intention. Products and services may be country-specific designed. All other mentioned company and software designations are trade marks or unregistered trade marks of the respective organizations and are liable to the corresponding legal regulations.

- The information in this document is proprietary to SEEBURGER. No part of this document may be reproduced, copied, or transmitted in any form or purpose without the express prior written permission of SEEBURGER AG.
- This document is a preliminary version and not subject to your license agreement or any other agreement with SEEBURGER. This document contains only intended strategies, developments, and functionalities of the SEEBURGER product and is not intended to be binding upon SEEBURGER to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SEEBURGER at any time without notice.
- SEEBURGER assumes no responsibility for errors or omissions in this document. SEEBURGER does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
- SEEBURGER shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
- The statutory liability for personal injury and defective products is not affected. SEEBURGER has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party web pages nor provide any warranty whatsoever relating to third-party web pages.