TÜVNORD

Inspired by
Knowledge

Teilnahmebescheinigung

Philip Knoll

hat an der Veranstaltung

Schulung: DORA-Verordnung in Unternehmen umsetzen

Alles Wichtige zur DORA-Verordnung – Anforderungen, Umsetzung und Auswirkungen für Ihr Unternehmen

(Seminarinhalte siehe Rückseite)

am 28.03.2025 teilgenommen
(Schulungsdauer 6 Unterrichtseinheiten).

Hamburg, 01.04.2025

TÜV NORD Akademie

Dr. Roland Bursy

Geschäftsführer

TÜV NORD Akademie GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg
tuevnordakademie.de

TÜV®

TÜVNORDGROUP

Inspired by Knowledge

Es wurden folgende Themen behandelt:

Gesamtüberblick DORA-Verordnung und weitere Informationssicherheitsgesetze im Kontext (DORA-Richtlinie, NIS-2, FinmadiG, Datenschutz)

Referentenentwurf Finanzmarktdigitalisierungsgesetz (FinmadiG): nationale Konkretisierungen zur Umsetzung der DORA in Deutschland

- Änderungen im Versicherungsaufsichtsgesetz (VAG), Kreditwesengesetz (KWG), Wertpapierhandelsgesetz (WpHG)
- Befugnisse der BaFin im Zusammenhang mit DORA
- Umsetzung der durch DORA geforderten Meldepflichten für IKT-Vorfälle
- Erweiterung der Jahresabschlussprüfung für Versicherungen (§ 35 Nr. 10 VAG)

Mitgeltende Dokumente

- Technische Regulierungsstandards (RTS)
- Technische Implementierungsstandards (ITS)
- Delegierte Rechtsakte

Überblick DORA-Verordnung

Begriffliche Definitionen

- „digitale operationale Resilienz"
- „kritische oder wichtige Funktion" vs. „wesentliche Auslagerung"

Berufsgeheimnis

Einschlägigkeit – wen betrifft die DORA-Verordnung?

- Proportionalitätsprinzip
- Ausnahmen und Erleichterungen u. a. Klein- u. Kleinstunternehmen (Art. 16, Abs. 5-16)
- Sektorspezifische Regulierung – Zusammenhang zur NIS-2-RL

Verhältnis DORA zu BAIT und VAIT

IT-Governance – Pflichten und Verantwortung der Geschäftsleitung bzw. Leitungsorgane (Art. 5 Abs. 2)

IKT-Risikomanagementrahmen

- Informationssicherheitsmanagementsystem (ISMS)
- Physische Umwelt
- „Identifizierung": Anforderungen an die Aufbau- und Ablauforganisation

Schulungspflicht der Leitungsorgane (Art. 5 Abs. 4)

Drittparteien-Risikomanagement

- Vertragliche Pflichten, § Handlungsbedarfe: § 25b KWG vs. Art. 30 DORA-VO
- Synergien: Berührungspunkte zu Auftragsverarbeitung und IT-Lieferkette gem. NIS-2
- Kontrollpflichten
- Kritische IKT-Dienstleister

Anforderungen an die IKT-Systeme, IKT-Sicherheit und IT Continuity

TOMs

- Backups und Wiederherstellung, Wiederanlaufpläne
- Redundanzen
- Weiterentwicklung

Cybersicherheitstests: Thread-Led Penetration Testing (TLPT)

IKT-Vorfälle

- Klassifizierung
- Prozess
- Meldung
- Kommunikation

Informationsaustausch

Befugnisse der Behörden

- Rolle der BaFin
- Zusammenarbeit
- Sanktionen
- Zwangsgelder für kritische IKT-Dienstleister (ErwG 81, Art. 35)