TRÖBER®
rechtsanwaltskanzlei

WHITEPAPER CYBER SECURITY:

HAFTUNGSRISIKEN DURCH IT-SICHERHEITSVORFÄLLE

VERANTWORTLICHKEIT UND HAFTUNG DER UNTERNEHMENSLEITUNG GEGENÜBER DER GESELLSCHAFT

EINRICHTUNGSPFLICHT FÜR ÜBERWACHUNGSSYSTEM

z. B. § 91 Abs. 2 AktG wonach der Vorstand verpflichtet wird

> *„geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden “*

Gilt häufig **auch für Geschäftsführer einer GmbH**, insbesondere wenn dort ein mitbestimmter oder fakultativer Aufsichtsrat existiert.

UNMITTELBARE RECHTSPFLICHTEN

Organisations- bzw. Überwachungs-pflichten aus **zwingendem Recht**.

z.B. **Datenschutzrecht**

Gewährleistung der Daten- und Systemsicherheit durch organisatorische und technische Maßnahmen (Art. 24, 25, 32 und 35 DS-GVO, ggf. § 64 BDSG)

ORGANISATIONSVERSCHULDEN

Fehlende oder unzureichende Organisation der Binnenstruktur der Gesellschaft
→ **„Compliance-Verstöße“**

z.B. § 93 Abs. 2 AktG, § 43 Abs. 2 GmbHG

TRÖBER® rechtsanwälte

VERANTWORTLICHKEIT UND HAFTUNG DER UNTERNEHMENSLEITUNG GEGENÜBER KUNDEN

DIREKTER SCHADENERSATZANSPRUCH

gegen Vorstand und Aufsichtsrat, soweit diese von der Gesellschaft keine Befriedigung erlangen können (§ 93 Abs. 5 AktG). In diesem Fall besteht eine persönliche Haftung des Vorstandes gegenüber den Gläubigern der Gesellschaft.

z. B.

ART. 82 DS-GVO

wegen Verletzung der Pflicht zur Einrichtung geeigneter technischer und organisatorischer Maßnahmen.

VERANTWORTLICHKEIT UND HAFTUNG DER GESELLSCHAFT GEGENÜBER KUNDEN

AUS VERTRAG

Durch Unterlassen der Einrichtung eines Überwachungssystems aus Vertrag wegen Verletzung einer vertraglichen Haupt- oder Nebenpflicht, § 280 BGB.

AUS GESETZ

- z. B. durch vorsätzliche oder fahrlässige Verletzung von Rechtsgütern der Kund*innen aus § 823 Abs. 1 BGB.
- z. B. aus Art. 82 DS-GVO

VERANTWORTLICHKEIT UND HAFTUNG DER GESELLSCHAFT WEGEN BUSSGELDERN & STRAFBARKEIT

DS-GVO

bei Datenschutzverstößen Bußgelder von bis zu **20 Millionen Euro** oder von bis zu vier Prozent des weltweiten Jahresumsatzes vor (je nachdem, welcher Betrag am Ende höher ist)

KRITIS, BSIG

Bis zu **1 Million Euro** bei nicht angemessenen TOM für Betreiber kritischer Infrastrukturen, §§ 14 Abs. 5, 8a Abs. 1 BSIG.

STGB

z.B. **Freiheitsstrafe bis zu drei Jahren** oder Geldstrafe bei **Unterstützung einer kriminellen Vereinigung** durch Lösegeldzahlung bei Ransomware Attack, § 129 Abs. 1 S. 2 StGB