Bennert
CONSULTING

# NIS2 Quick Check

## Die 7 Pflichten, die jeder erfüllen muss.

In einfacher Sprache. Mit Prüfkriterien, typischen Lücken und Sofort-Aktionen.

12 Seiten. Direkt aus der Praxis.

---

Herausgeber: Bennert Consulting

Stand: 2026

> **Bonus im Paket**
>
> Nach dem Download ist Ihr Zugang zum NIS2 Mini Kurs freigeschaltet. 3 Videomodule, je 10 Minuten.

# Wer sollte das lesen

Dieses Dokument richtet sich an Entscheider im Gesundheitswesen, die sich selbst einen ehrlichen Status verschaffen wollen, ohne Gesetzestext und ohne Beraterfolie.

## Lesen Sie dieses Dokument, wenn Sie:

- Geschäftsführung eines Unternehmens im Gesundheitswesen sind
- IT-Leitung oder IT-Sicherheitsverantwortlicher in einer Gesundheitseinrichtung sind
- für die NIS2-Umsetzung Ihrer Einrichtung verantwortlich sind
- wissen wollen, was der Prüfer von Ihnen verlangt
- nicht noch einen 80-Seiten-Leitfaden lesen wollen

## Was Sie nach 30 Minuten Lesezeit wissen:

- Die 7 Pflichten, die Ihr Unternehmen erfüllen muss
- Die Kriterien, auf die der Prüfer schaut
- Die 3 Lücken, die bim Gesundheitswesen bei der Prüfung am häufigsten auffallen
- Was Sie ab morgen konkret tun können

## Inhalt

# Warum NIS2 jetzt nicht mehr aufgeschoben werden kann

NIS2 gilt in Deutschland seit der Umsetzung im NIS2UmsuCG. Die Frist ist verstrichen. Prüfungen laufen bereits.

Wenn Sie bis heute gehofft haben, dass sich das Thema noch verschiebt, dann ist diese Hoffnung vorbei.

**Es gibt drei Gründe, warum das Thema bei Ihnen sofort auf den Tisch gehört.**

## 1. Persönliche Haftung der Geschäftsführung

NIS2 ist das erste Informationssicherheitsgesetz in Deutschland, das die Geschäftsführung persönlich in die Pflicht nimmt. Das bedeutet: Wenn ein Sicherheitsvorfall eintritt und Sie nicht nachweisen können, dass Sie die erforderlichen Maßnahmen ergriffen haben, kann das persönliche Folgen für Sie haben.

Nicht für die IT-Abteilung. Nicht für den Datenschutzbeauftragten. Sondern für Sie als Geschäftsführer oder Vorstand.

## 2. Bußgelder

Die Bußgelder nach NIS2 gehen bis zu 10 Mio. Euro oder 2 Prozent vom weltweiten Jahresumsatz. Es gilt der höhere Wert.

Beispiel: Für einen Klinikverbund mit mehreren hundert Millionen Euro Jahresumsatz kann das Bußgeld also deutlich über 10 Mio. Euro hinausgehen.

## 3. Versorgungsrelevanz

Im Gesundheitswesen geht es bei NIS2 nicht nur um IT-Systeme. Es geht um Patientenversorgung.

Wenn Ihre Systeme durch einen Ransomware-Angriff ausfallen, können Sie keine Patientendaten einsehen. Keine Medikamente verschreiben. Keine OPs planen. Die Notaufnahme kann nicht arbeiten.

Das ist keine theoretische Gefahr. Das ist passiert. Mehrfach im ganzen deutschen Gesundheitssektor.

NIS2 fordert explizit, dass Sie solche Szenarien bewertet, dokumentiert und abgesichert haben.

## Die gute Nachricht

Die Anforderungen sind strukturiert. NIS2 definiert 7 Pflichten. Wenn Sie diese 7 verstanden haben, haben Sie den Kern.

Die folgenden 7 Seiten nehmen Sie jede Pflicht einzeln durch. Mit konkreten Beispielen aus dem Alltag. Mit den Kriterien, die der Prüfer sehen will. Mit den Lücken, die im deutschen Gesundheitssektor am häufigsten auffallen.

# Pflicht 1: Ein dokumentiertes Sicherheitskonzept

> **Was NIS2 verlangt:** Ein schriftliches Sicherheitskonzept, das von der Geschäftsführung freigegeben ist und regelmäßig aktualisiert wird.

## Was das konkret bedeutet

In Ihrerm Unternehmen gibt es eine offizielle Linie, wie mit sensiblen Daten, IT-Systemen und versorgungskritischen Prozessen umgegangen wird. Das Dokument muss drei Dinge erfüllen: aktuell sein, bekannt sein, und die Unterschrift der Geschäftsführung tragen.

Kein 80-Seiten-Dokument. Ein klares Papier, das beschreibt, was bei Ihnen gilt.

## Was der Prüfer sehen will

- Ein aktuelles Sicherheitskonzept, nicht älter als 12 Monate
- Nachweisbare Freigabe durch die Geschäftsführung (Unterschrift oder Vorstandsbeschluss)
- Klare Benennung der klinischen IT-Systeme, die geschützt werden (KIS, RIS, LIS, Medikamentenmanagement, Patientenportal)
- Regelmäßige Überprüfung, dokumentiert mit Datum und Verantwortlichem
- Definierte Schutzziele: Verfügbarkeit, Unveränderlichkeit, Vertraulichkeit

## Die typische Lücke im Gesundheitswesen

Es gibt ein Sicherheitskonzept von vor drei Jahren. Es wurde formal nie von der Geschäftsführung freigegeben. Die patientennahen Systeme werden nicht explizit genannt. Außer der IT-Leitung kennt es niemand.

Der Prüfer fragt danach und Sie legen ein Dokument vor, das offensichtlich Aktenschrankware ist.

## Was Sie jetzt tun können

1. Prüfen Sie, ob Ihr aktuelles Sicherheitskonzept schriftlich vorliegt.
2. Prüfen Sie, ob es von der Geschäftsführung freigegeben ist (Unterschrift oder Vorstandsprotokoll).
3. Prüfen Sie, ob es die wichtigsten klinischen IT-Systeme namentlich nennt.

Wenn eine dieser drei Voraussetzungen fehlt, ist das Ihre erste Baustelle.

# Pflicht 2: Risiken bewerten und behandeln

> **Was NIS2 verlangt:** Eine strukturierte Bewertung der Risiken für Ihre IT-Systeme und versorgungskritischen Prozesse, inklusive Maßnahmen zur Risikoreduktion.

## Was das konkret bedeutet

Sie müssen wissen, was in in ihrem Unternehmen schiefgehen kann. Nicht als Bauchgefühl. Als dokumentierte Bewertung.

Für jeden wichtigen Prozess und jedes kritische System: Was könnte ausfallen? Wie wahrscheinlich ist das? Wie schwer wären die Folgen? Was tun Sie, um das zu verhindern?

## Was der Prüfer sehen will

- Eine Liste aller versorgungskritischen Prozesse und Systeme
- Für jeden Eintrag: bewertete Risiken mit Wahrscheinlichkeit und Auswirkung
- Für jedes Risiko: eine dokumentierte Entscheidung (Maßnahme, akzeptieren, übertragen)
- Die Restrisiken sind durch die Geschäftsführung akzeptiert
- Regelmäßige Überprüfung, mindestens jährlich

## Die typische Lücke im Gesundheitswesen

Es gibt eine Risikoliste aus einer Qualitätsmanagement-Revision. Sie enthält allgemeine Risiken wie Brand und Stromausfall. Aber keine konkreten IT-Risiken. Kein Eintrag zum Ausfall kritischer Systeme. Kein Eintrag zur Ransomware. Kein Eintrag zu Medikamentenlieferanten etc.

Und selbst wenn Risiken erfasst sind: Es gibt keine dokumentierte Behandlungsentscheidung. Die Risiken stehen da. Niemand hat entschieden, was damit zu tun ist.

## Was Sie jetzt tun können

1. Erstellen Sie eine einfache Tabelle mit Ihren 10 wichtigsten klinischen IT-Systemen.
2. Für jedes System: Was passiert, wenn es für 24 Stunden ausfällt? Für 72 Stunden?
3. Dokumentieren Sie für jedes Risiko eine Entscheidung: Was tun Sie dagegen, oder akzeptieren Sie es bewusst?

# Pflicht 3: Umgang mit Sicherheitsvorfällen

> **Was NIS2 verlangt:** Einen dokumentierten Prozess für den Umgang mit Sicherheitsvorfällen, inklusive der Meldung an das BSI innerhalb gesetzlicher Fristen.

## Was das konkret bedeutet

Wenn in Ihrerem Unternehmen etwas passiert – ein Ransomware-Angriff, ein Datenleck, ein Systemausfall durch einen Angriff – dann muss klar sein: Wer informiert wen? Wer meldet an das BSI? Wer dokumentiert was?

NIS2 setzt kurze Fristen: Die erste Meldung an das BSI muss innerhalb von **24 Stunden** erfolgen. Eine ausführliche Bewertung innerhalb von **72 Stunden**. Ein Abschlussbericht innerhalb eines Monats.

## Was der Prüfer sehen will

- Ein dokumentierter Prozess für den Umgang mit Sicherheitsvorfällen
- Klare Definition, was überhaupt als Sicherheitsvorfall gilt (Klassifikation)
- Meldewege bis zur Geschäftsführung, namentlich benannt
- Meldeformulare oder Vorlagen für die BSI-Meldung
- Nachweis, dass der Prozess mindestens einmal geübt wurde (Übung oder realer Vorfall)

## Die typische Lücke im Gesundheitswesen

Es gibt einen IT-Notfallplan von 2019. Er beschreibt, wen man bei einem Serverausfall ruft. Aber nicht, wer die BSI-Meldung schreibt. Nicht, wer innerhalb der 24-Stunden-Frist die Geschäftsführung informiert. Nicht, wie ein Ransomware-Fall vom bloßen Systemfehler unterschieden wird.

Wenn der Ernstfall eintritt, diskutieren fünf Leute im Meeting, wer jetzt eigentlich was meldet.

## Was Sie jetzt tun können

1. Legen Sie eine Eskalationskette auf einer Seite fest: Wer meldet bei Verdacht an wen? Mit Namen und Telefonnummern.
2. Dokumentieren Sie einen einfachen Entscheidungsbaum: Ab wann ist es ein Sicherheitsvorfall nach NIS2?
3. Proben Sie das Szenario einmal mit Ihrer IT-Leitung. Halten Sie die Probe schriftlich fest.

# Pflicht 4: Notfallplan für Ausfälle

> **Was NIS2 verlangt:** Einen Plan, wie Ihre Einrichtung den Betrieb aufrechterhält, wenn wichtige Systeme oder Lieferanten ausfallen.

## Was das konkret bedeutet

Im Gesundheitswesen ist das die Kernfrage. Wenn Ihr KIS für 48 Stunden ausfällt: Wie versorgen Sie Ihre Patienten weiter? Welche Prozesse müssen weiterlaufen, auch wenn die IT steht?

Der Plan muss schriftlich vorliegen. Er muss realistische Wiederanlaufzeiten definieren. Und er muss regelmäßig getestet werden.

## Was der Prüfer sehen will

- Eine Liste der versorgungskritischen Prozesse in Ihrer Einrichtung (Notaufnahme, OP, Medikamentenausgabe, Labor, etc.)
- Für jeden Prozess: Wie lange können wir ohne IT auskommen? Welche Systeme müssen wie schnell wieder laufen?
- Einen schriftlichen Notfallplan für die wichtigsten Szenarien (KIS-Ausfall, Stromausfall, Ransomware)
- Dokumentierte Wiederherstellungsübungen mit Datum und Ergebnis
- Mindestversorgungsniveaus: Was ist das Minimum, das wir halten müssen, auch im schlimmsten Fall?

## Die typische Lücke im Gesundheitswesen

Es gibt Papierformulare für den Notfall. Theoretisch. In der Schublade der Stationsleitung, die aktuell krank ist. Niemand weiß, wo der Ordner wirklich liegt. Eine Wiederherstellungsübung hat es seit drei Jahren nicht gegeben.

Wenn gefragt wird, wie lange die Notaufnahme ohne KIS arbeiten kann, antwortet die IT-Leitung mit „eine Weile schon", die Ärztliche Leitung mit „zwei Stunden maximal". Beide haben unrecht.

## Was Sie jetzt tun können

1. Identifizieren Sie Ihre 5 wichtigsten Prozesse: Welche dürfen unter keinen Umständen ausfallen?
2. Legen Sie für jeden Prozess eine maximal tolerierbare Ausfallzeit fest.
3. Planen Sie innerhalb der nächsten 3 Monate eine kurze Wiederherstellungsübung.

# Pflicht 5: Sicherheit in der Lieferkette

> **Was NIS2 verlangt:** Sie müssen Ihre kritischen Lieferanten und deren Unter-Lieferanten bewerten und absichern.

## Was das konkret bedeutet

Das ist die Pflicht, die im Gesundheitswesen am stärksten unterschätzt wird. Ihre Einrichtung arbeitet mit Medikamentenlieferanten, Medizintechnikherstellern, externen Laboren, IT-Dienstleistern. Diese Lieferanten arbeiten selbst wieder mit Lieferanten, die Sie nie gesehen haben.

Wenn einer davon ausfällt oder kompromittiert wird, kann das Ihre Patientenversorgung stoppen. NIS2 verlangt, dass Sie diese Lieferkette bis zur dritten Ebene bewertet haben.

## Was der Prüfer sehen will

- Eine Liste Ihrer kritischen Lieferanten mit Priorität
- Für jeden kritischen Lieferanten: eine Bewertung des Risikos
- Vertragliche Informationssicherheitsanforderungen in den Lieferantenverträgen
- Dokumentierte Abhängigkeiten, auch zu Unter-Lieferanten
- Eine Strategie für den Ausfall kritischer Lieferanten (Alternativen, Ersatzquellen)

## Die typische Lücke im Gesundheitswesen

Es gibt einen Hauptlieferanten für Medikamente. Was den dahinter antreibt, weiß niemand. Welche UnterLieferanten der Medizintechnikhersteller nutzt, ist nie bewertet worden. Für den Ausfall des IT-Dienstleisters gibt es keinen Plan B.

Der Prüfer fragt: Was passiert, wenn Ihr Hauptmedikamentenlieferant morgen pleite geht? Die Antwort ist meistens Schweigen.

## Was Sie jetzt tun können

1. Erstellen Sie eine Liste Ihrer 10 wichtigsten Lieferanten (Medikamente, Medizintechnik, IT, Energie).
2. Bewerten Sie für jeden: Wie kritisch ist er? Gibt es Alternativen?
3. Prüfen Sie für die 3 kritischsten Lieferanten, welche Unter-Lieferanten sie selbst nutzen.

# Pflicht 6: Zugriffe kontrollieren

> **Was NIS2 verlangt:** Zugriffe auf wichtige Systeme müssen besonders geschützt und regelmäßig überprüft sein.

## Was das konkret bedeutet

Im Gesundheitswesenhaben viele Menschen Zugriff auf sensible Systeme: angestellte Ärzte, Pflegekräfte, externe Bereitschaftsärzte, Reinigungsdienste, IT-Dienstleister, Wartungsfirmen für Medizintechnik.

NIS2 verlangt: Sie müssen wissen, wer Zugriff hat. Sie müssen das regelmäßig prüfen. Und besonders kritische Zugänge müssen zusätzlich abgesichert sein.

## Was der Prüfer sehen will

- Dokumentierte Berechtigungskonzepte für die wichtigsten Systeme
- Mehrfaktor-Authentisierung für privilegierte Zugriffe (Administratoren)
- Regelmäßige Überprüfung der Zugriffsrechte (mindestens jährlich)
- Protokollierung der Zugriffe auf sensible Daten
- Klarer Prozess für den Entzug von Berechtigungen bei Austritt oder Wechsel

## Die typische Lücke im Gesundheitswesen

Externe Bereitschaftsärzte haben seit 2021 ein KIS-Konto. Sie sind längst weg. Ihre Zugänge existieren noch. Die Reinigungsfirma hat Zugänge zu Räumen mit Servertechnik. Niemand hat das regelmäßig geprüft.

Die IT-Administratoren melden sich ohne Mehrfaktor-Authentisierung an. Ein einziges gestohlenes Passwort würde reichen.

## Was Sie jetzt tun können

1. Fordern Sie eine aktuelle Liste aller KIS-Benutzer. Prüfen Sie, wie viele davon seit mehr als 6 Monaten nicht eingeloggt waren.
2. Prüfen Sie, ob Ihre IT-Administratoren eine zweite Sicherheitsstufe beim Login nutzen.
3. Führen Sie einmal jährlich eine Berechtigungsrevision durch, dokumentiert mit Datum und Ergebnis.

# Pflicht 7: Schulung und Aufmerksamkeit

> **Was NIS2 verlangt:** Ihre Mitarbeitenden müssen regelmäßig zu Informationssicherheit geschult sein, angepasst an ihre Rolle.

## Was das konkret bedeutet

Ein Pflegemitarbeitender braucht andere Schulungsinhalte als die IT-Leitung. Ein angestellter Arzt andere als die Geschäftsführung. NIS2 verlangt: Schulungen müssen rollenspezifisch sein, regelmäßig stattfinden und dokumentiert werden.

Nicht ein einmaliges E-Learning beim Onboarding. Kontinuierliche Aufmerksamkeit für die realen Bedrohungen im Alltag von Gesundheitseinrichtungen.

## Was der Prüfer sehen will

- Ein Schulungskonzept mit Rollenzuordnung
- Nachweise, dass Schulungen tatsächlich stattgefunden haben (Teilnehmerlisten, Testergebnisse)
- Regelmäßigkeit (mindestens jährlich)
- Inhalte, die zu Ihrer Einrichtung passen (nicht generische E-Learnings)
- Nachweise für die Geschäftsführung selbst (ja, auch Sie müssen geschult werden)

## Die typische Lücke im Gesundheitswesen

Es gibt ein Onboarding-E-Learning. 45 Minuten. Jeder macht es einmal beim Einstieg. Danach nie wieder. Die Inhalte sind generisch, aus einem Katalog, ohne Bezug zu klinischen Szenarien. Die Geschäftsführung selbst hat die Schulung nie gemacht.

Wenn Phishing-Mails an Pflegekräfte gehen, klickt die Hälfte davon. Keine kennt die typischen Betrugsmuster.

## Was Sie jetzt tun können

1. Prüfen Sie, wann die letzte Informationssicherheitsschulung für Pflegepersonal stattgefunden hat.
2. Prüfen Sie, ob die Geschäftsführung selbst ebenfalls geschult wurde. Wenn nein: holen Sie das innerhalb der nächsten 30 Tage nach.
3. Planen Sie eine einfache Awareness-Kampagne zu Phishing und Passwortsicherheit. Ein 20-minütiges internes Video reicht, wenn es rollenspezifisch ist.

# Die 3 häufigsten Lücken im deutschen Gesundheitswesen

Wenn wir Vorprüfungen machen, sehen wir fast überall dieselben drei Lücken. Sie sind der Grund, warum später im echten Prüfverfahren die meisten Beanstandungen kommen.

## Lücke 1: Die Lieferkette bis zur dritten Ebene nicht dokumentiert

Unternehmen kennen ihre direkten Lieferanten. Aber nicht deren Lieferanten. Im Fall der Fälle ist völlig offen, wer wem zuarbeitet. NIS2 verlangt die Bewertung bis zur dritten Ebene. In 9 von 10 Fällen ist das nicht vorhanden.

## Lücke 2: Kein realistischer Notfallplan für KIS-Ausfälle über 24 Stunden

Der kurzfristige Ausfall ist oft gedacht. Der mehrtägige Ausfall fast nie. Wenn das KIS durch Ransomware 72 Stunden steht, bricht in den meisten Unternehmen die Dokumentation der wichtigsten Prozesse zusammen. Papier-Backups fehlen, Abläufe wurden nicht geprobt.

## Lücke 3: Berechtigungen von externen Dienstleistern und Bereitschaftsärzten nicht regelmäßig geprüft

Zugänge werden vergeben, aber selten geprüft. Externe Bereitschaftsärzte, Wartungsfirmen für Medizintechnik, ehemalige Mitarbeiter mit Restrechten: diese Zugänge akkumulieren sich. Der Prüfer findet das sofort, wenn er die Benutzerliste zieht.

## Ihr Selbst-Check in 10 Fragen

Beantworten Sie folgende Fragen mit Ja oder Nein. Je mehr Nein-Antworten, desto dringender ist Ihre Handlungsnotwendigkeit.

| # | Frage | Ja / Nein |
|---|---|---|
| 1 | Wir haben ein aktuelles Sicherheitskonzept, freigegeben von der Geschäftsführung innerhalb der letzten 12 Monate. | |
| 2 | Unsere 10 wichtigsten IT-Systeme sind in einer Risikobewertung erfasst, inklusive Behandlungsentscheidung. | |
| 3 | Es gibt einen schriftlichen Prozess für die Meldung von Sicherheitsvorfällen, inklusive BSI-Meldung. | |
| 4 | Die BSI-Meldekette wurde innerhalb der letzten 12 Monate einmal geübt. | |

| # | Frage | Ja / Nein |
|---|---|---|
| 5 | Wir haben für die 5 wichtigsten klinischen Prozesse eine maximal tolerierbare Ausfallzeit festgelegt. | |
| 6 | Wir haben eine bewertete Liste unserer 10 wichtigsten Lieferanten. | |
| 7 | Für unsere 3 kritischsten Lieferanten kennen wir deren Unter-Lieferanten. | |
| 8 | IT-Administratoren melden sich nur mit Mehrfaktor-Authentisierung an. | |
| 9 | Berechtigungen in wichtigen Systemen werden mindestens einmal jährlich überprüft. | |
| 10 | Die Geschäftsführung hat innerhalb der letzten 12 Monate eine Informationssicherheitsschulung absolviert. | |

### Auswertung

- **9 oder 10 mal Ja:** Sie sind gut aufgestellt. Eine Vorprüfung wird Details finden, aber keine strukturellen Lücken.
- **6 bis 8 mal Ja:** Sie haben die Basis gelegt. Gezielte Nacharbeit an 2 bis 4 Themen, dann sind Sie prüfungsbereit.
- **3 bis 5 mal Ja:** Ihre Grundlagen sind da, aber die Umsetzung ist unvollständig. Mit strukturierter Arbeit in 8 bis 12 Wochen machbar.
- **0 bis 2 mal Ja:** Akuter Handlungsbedarf. Die Prüfung würde aktuell mit erheblichen Beanstandungen enden.

# Nächste Schritte

Sie haben jetzt den Überblick. Sie wissen, was NIS2 von Ihrer Einrichtung verlangt, worauf der Prüfer schaut, und wo die typischen Lücken liegen.

Die Frage ist: Wie gehen Sie es an?

## Option 1: Selbst umsetzen

Wenn Ihr Selbst-Check mindestens 7 Ja-Antworten ergeben hat und Sie interne Ressourcen haben: Arbeiten Sie die 7 Pflichten der Reihe nach ab. Unser NIS2 Mini Kurs (3 Videomodule) gibt Ihnen den inhaltlichen Rahmen.

→ **Jetzt zum NIS2 Mini Kurs** *[Link in der E-Mail, die Sie erhalten haben]*

## Option 2: Prüfen, wo Sie wirklich stehen

Wenn Sie unsicher sind, ob Ihr Selbst-Check die Realität abbildet: Nutzen Sie unsere kostenlose Potenzialanalyse. 30 Minuten. Unverbindlich.

Wir schauen gemeinsam auf Ihren Status in den 7 Pflichtbereichen. Wir zeigen Ihnen, welche Lücken in der echten Prüfung auffallen würden. Und wir machen Ihnen einen konkreten Vorschlag, ob und wie wir Sie unterstützen können.

Kein Pitch. Kein Druck. Eine ehrliche Einschätzung.

→ **Kostenlose Potenzialanalyse buchen** *[Link in der E-Mail, die Sie erhalten haben]*

## Über Bennert Consulting

Bennert Consulting begleitet KRITIS-Betreiber und Gesundheitseinrichtungen durch NIS2-Prüfungen. Wir kennen die Fragen, die der Prüfer stellt, weil wir selbst Prüfungen vorbereiten, begleiten und verteidigen.

Unsere Kunden:

- Klinik Darmstadt
- Klinikum Hanau
- Noweda e.G.AOK
- AOK
- weitere Einrichtungen im Gesundheits- und Versorgungssektor

Was uns auszeichnet: Keine Beraterfolien. Keine 80-Seiten-Theorie. Direkte Umsetzung mit Vorlagen, die der Prüfer akzeptiert.

## Kontakt

Bennert Consulting
Marc Bennert
marc@bennert-consulting.de | +49 175 41 65 823
bennertconsulting.de

---

*Dieses Dokument ist eine allgemeine Orientierungshilfe zu den NIS2-Pflichten im Gesundheitswesen und ersetzt keine individuelle Rechts- oder Fachberatung.*