TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"TeleTrusT-Konferenz 2021"

Berlin, 25.11.2021

IT-Sicherheitsgesetz 2.0

Einordnung und Wirkungen

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte, Vorstand TeleTrusT, Leiter AG Recht

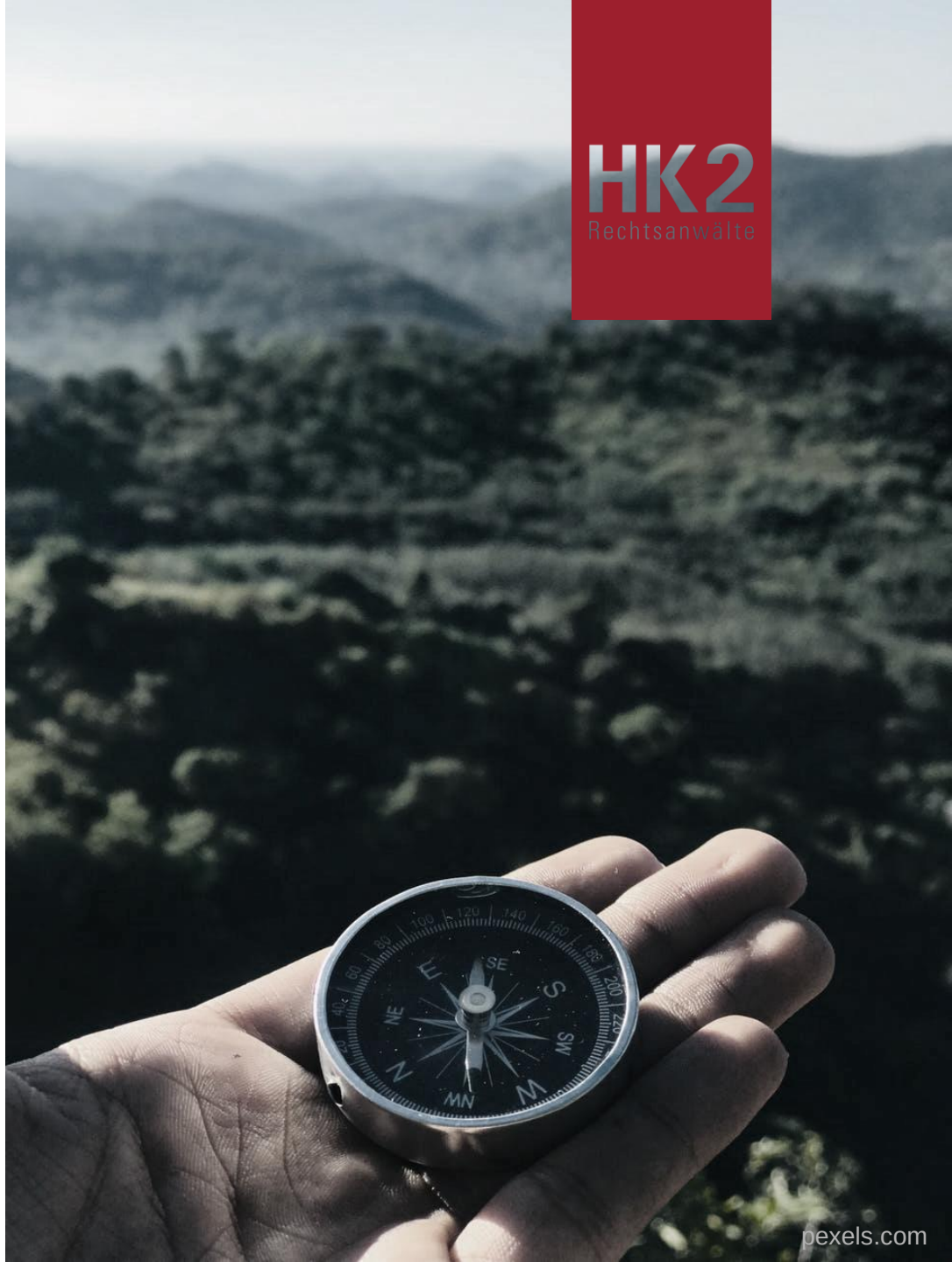
… to be discussed

1. Einordnung und Ausblick
2. Hersteller und UBI
3. Wirkungen auf Parteien und Verträge

HK2 Rechtsanwälte

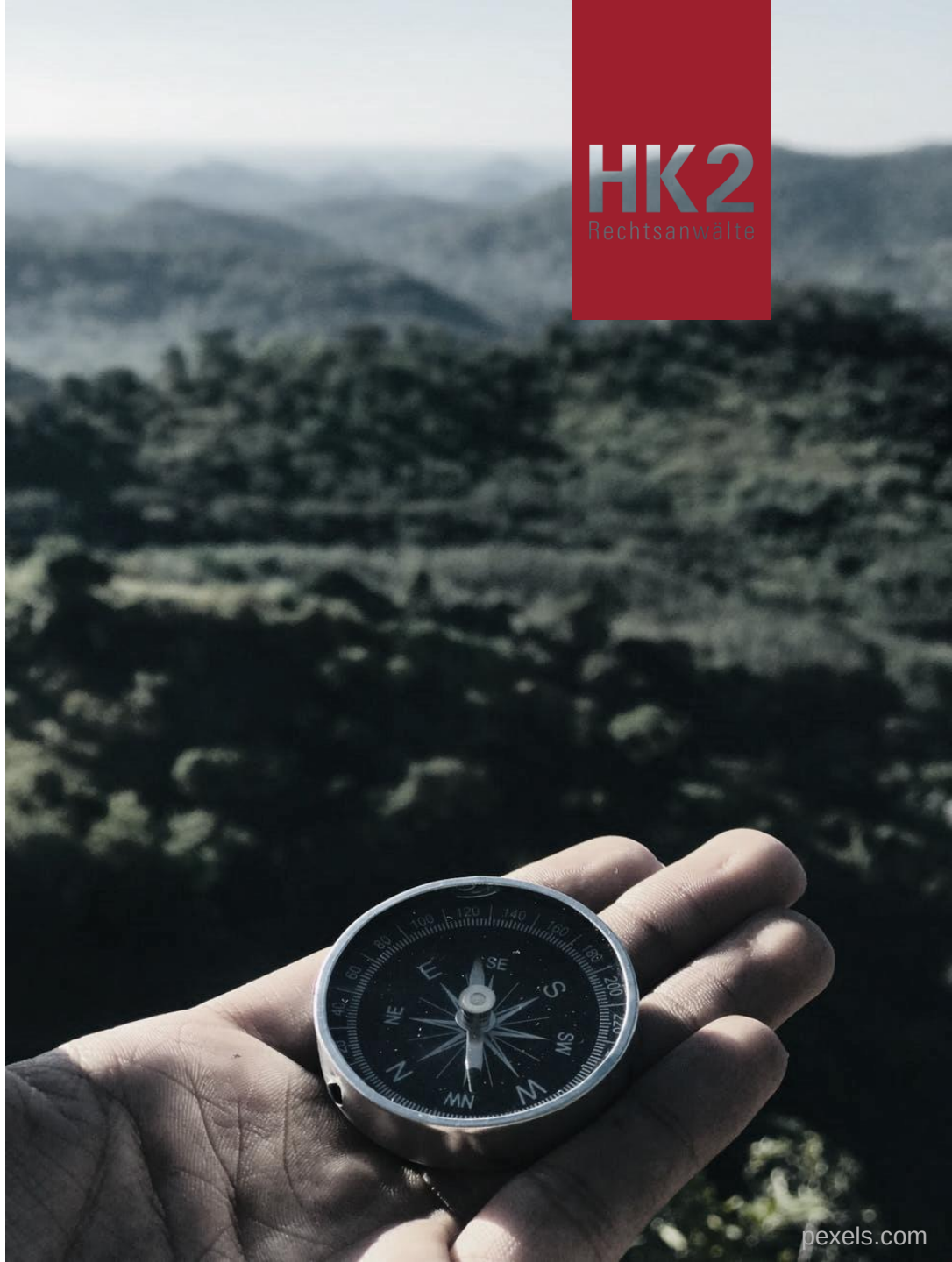
Eliot Sloman/Unsplash

Einordnung und Ausblick



Einordnung und Ausblick

1. Anwendungsbereich
2. EU NIS-2-Richtlinie
3. Rolle und Befugnisse des BSI
4. IT-Sicherheitskennzeichen (§ 9c BSIG)
5. Herstellerhaftung



Antwort der Bundesregierung auf Kleine Anfrage Drucksache 19/27487 v. 10.03.2021, S. 11

HK2 Rechtsanwälte

Erkennt die Bundesregierung, auch mit Blick auf den aktuellen Fall, Probleme bei der Herstellerhaftung?

Wenn ja, wie will sie diesen konkret gesetzgeberisch begegnen, und welche Maßnahmen enthält das „IT-Sicherheitsgesetz 2.0“ (ITSiG2.0) hierzu?

Wenn nein, warum nicht?

Antwort der Bundesregierung auf Kleine Anfrage Drucksache 19/27487 v. 10.03.2021, S. 11

HK2 Rechtsanwälte

Antwort:

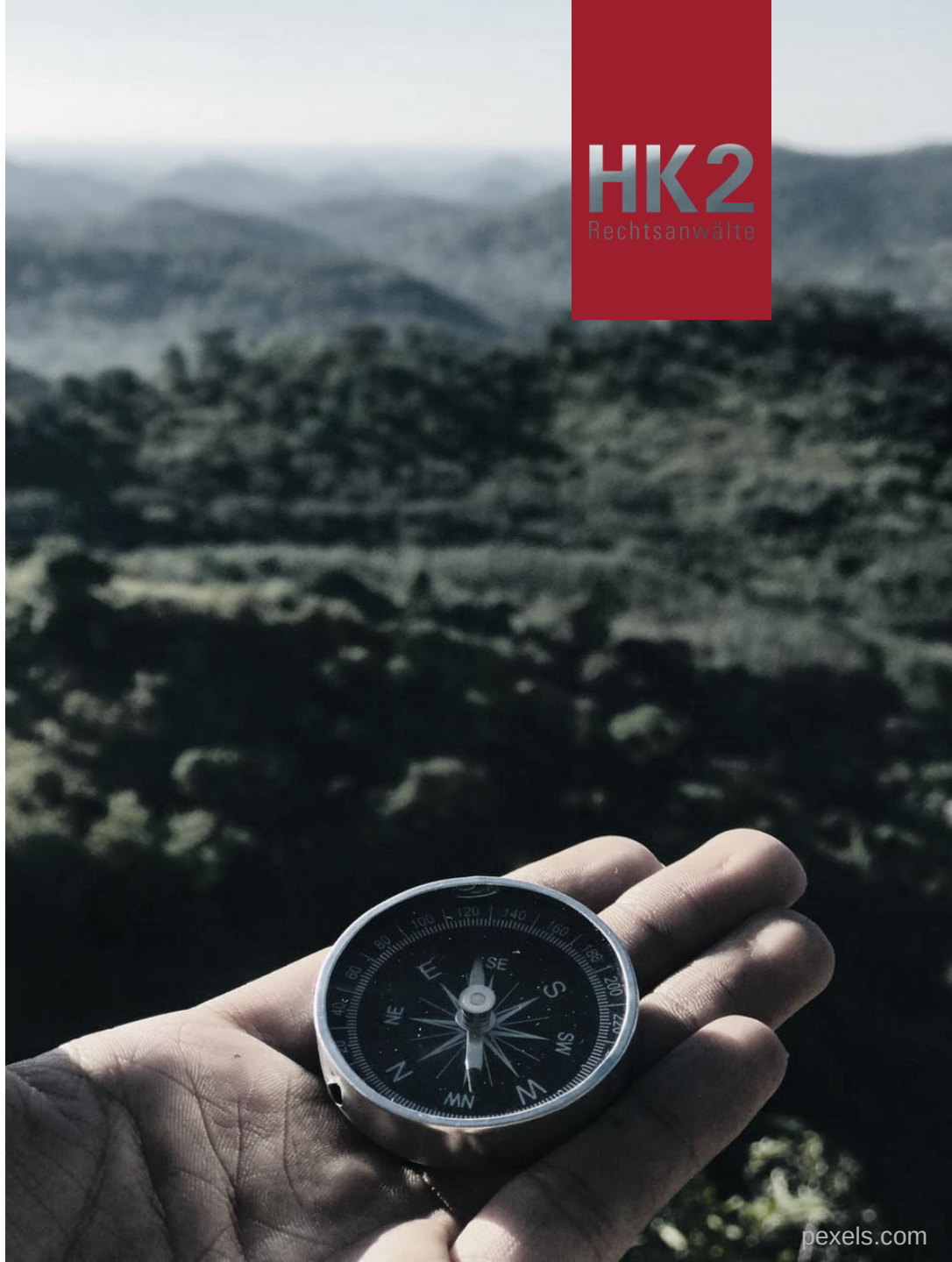
… Aufgrund der Vollharmonisierung dieses Rechtsgebiets sind gesetzgeberische Reformen nur auf europäischer Ebene möglich…

Eine punktuelle Überarbeitung der Produkthaftungsrichtlinie ist insoweit im Zuge des Revisionsprozesses zu prüfen, für den die EU-Kommission einen Vorschlag in diesem Jahr angekündigt hat

… das IT-Sicherheitsgesetz 2.0 als nationale Regelungsvorschrift [ist] im Übrigen nicht der richtige Standort für derartige gesetzliche Regelungen.

Einordnung und Ausblick

1. Anwendungsbereich
2. NIS-2-Richtlinie
3. Rolle und Befugnisse des BSI
4. IT-Sicherheitskennzeichen (§ 9c BSIG)
5. Herstellerhaftung
6. Stand der Technik



§ 8a Abs. 1a BSIG-ENT (ITSiG 2.0 RefENT, Mai 2020)

HK2 Rechtsanwälte

„… Die eingesetzten Systeme zur Angriffserkennung ***haben dem jeweiligen Stand der Technik zu entsprechen****. Die* ***Einhaltung des Standes der Technik wird vermutet, wenn*** *die Systeme* ***der Technischen Richtlinie [Bezeichnung] des Bundesamtes*** *in der jeweils geltenden Fassung* ***entsprechen****.*

HK2 Rechtsanwälte

§ 3 Abs. 1 Ziff. 20 BSIG (Aufgaben des BSI)

*„**Beschreibung** und Veröffentlichung **eines Stands der Technik** bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.“*

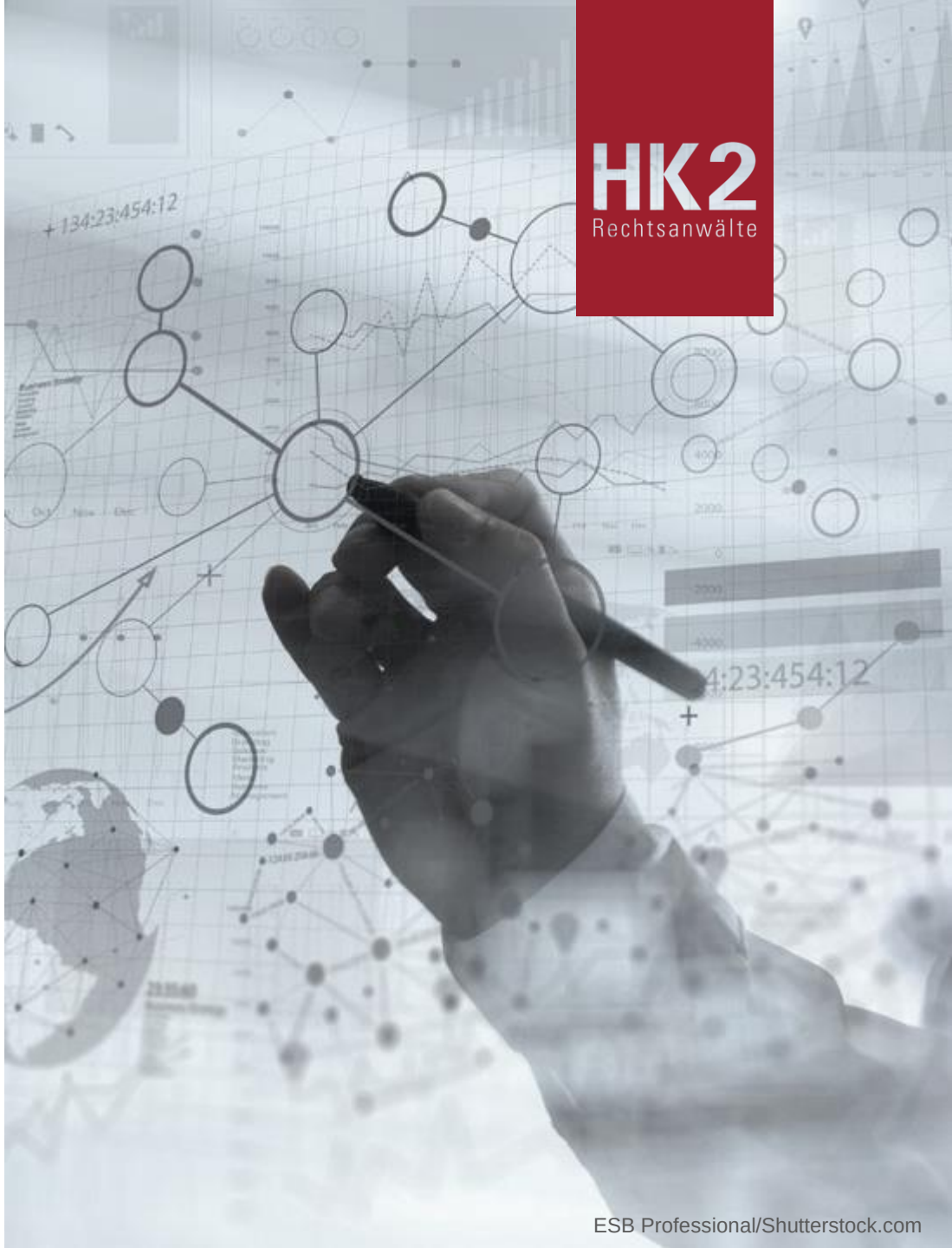
HK2 Rechtsanwälte

Für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG gilt:

§ 8f Abs. 3 BSIG (IT-Sicherheit in UBI)

„Das Bundesamt kann auf Grundlage der Selbsterklärung nach Absatz 1 ***Hinweise*** *zu angemessenen* ***organisatorischen und technischen Vorkehrungen*** *nach Absatz 1 Nummer 3 zur Einhaltung des* ***Stands der Technik*** *geben.“*

Hersteller kritischer Komponenten



ESB Professional/Shutterstock.com

HK2 Rechtsanwälte

Hersteller kritischer Komponenten

- Kritische Komponenten im Sinne von § 2 Ziff. 13 BSIG sind IT-Produkte
  - die **in Kritischen Infrastrukturen eingesetzt** werden (Nr. 1),
  - bei denen **Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit **zu** einem **Ausfall** oder zu einer **erheblichen Beeinträchtigung** der Funktionsfähigkeit Kritischer Infrastrukturen oder zu **Gefährdungen** für die öffentliche Sicherheit **führen können** (Nr. 2) **und**
  - die **gesetzlich als „kritische Komponente“** bestimmt oder eine gesetzlich definierte **„kritischen Funktion“ realisieren** (Nr. 3).

Einsatz kritischer Komponenten durch KRITIS-Betreiber

HK2 Rechtsanwälte

§ 9b Abs. 3 BSIG Untersagung des Einsatzes kritischer Komponenten

- S. 1: Einsatz *kritischer Komponenten* nur zulässig, wenn **Hersteller** eine Erklärung über seine Vertrauenswürdigkeit (**Garantieerklärung**) **gegenüber dem KRITIS-Betreiber** abgeben hat.

- S. 3: Garantieerklärung enthält Angaben dazu, **wie** der Hersteller **sicherstellt**, dass die kritische Komponente **nicht über technische Eigenschaften verfügt**, die spezifisch geeignet sind, **missbräuchlich**, insbesondere zum Zwecke von **Sabotage**, **Spionage** oder **Terrorismus** auf die **Sicherheit**, **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** oder **Funktionsfähigkeit** der Kritischen Infrastruktur einwirken zu können.

- S. 4: BMI legt Einzelheiten der Mindestanforderungen an die Garantieerklärung durch Allgemeinverfügung (Bundesanzeiger) fest.

HK2
Rechtsanwälte

Gesetzliche Anforderungen an Einsatz kritischer Komponenten führen zu **faktischen Obliegenheiten** und **vertraglichen Verpflichtungen des Herstellers**.

Einsatz kritischer Komponenten durch KRITIS-Betreiber

HK2 Rechtsanwälte

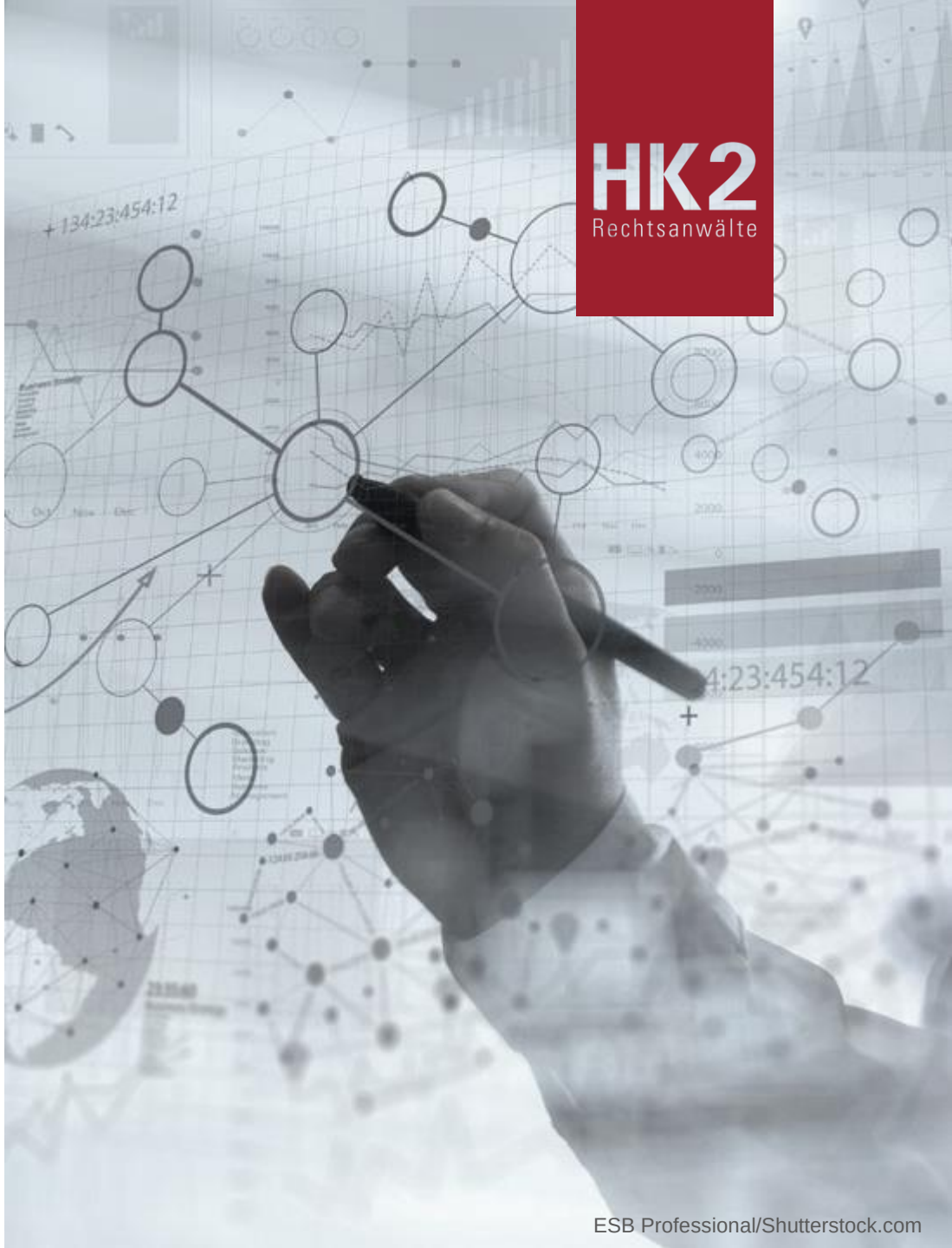
§ 9b Abs. 3 BSIG Untersagung des Einsatzes kritischer Komponenten

- S. 1: Einsatz *kritischer Komponenten* nur zulässig, wenn Hersteller eine Erklärung über seine Vertrauenswürdigkeit (**Garantieerklärung**) gegenüber dem KRITIS-Betreiber abgeben hat.

- S. 3: Garantieerklärung enthält Angaben dazu, **wie** der Hersteller **sicherstellt**, dass die kritische Komponente **nicht über technische Eigenschaften verfügt**, die spezifisch geeignet sind, **missbräuchlich**, insbesondere zum Zwecke von **Sabotage**, **Spionage** oder **Terrorismus** auf die **Sicherheit**, **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** oder **Funktionsfähigkeit** der Kritischen Infrastruktur einwirken zu können.

- S. 4: BMI legt Einzelheiten der Mindestanforderungen an die Garantieerklärung durch Allgemeinverfügung (Bundesanzeiger) fest.

Hersteller
von IT-Produkten



ESB Professional/Shutterstock.com

Hersteller informationstechnischer Produkte und Systeme

HK2 Rechtsanwälte

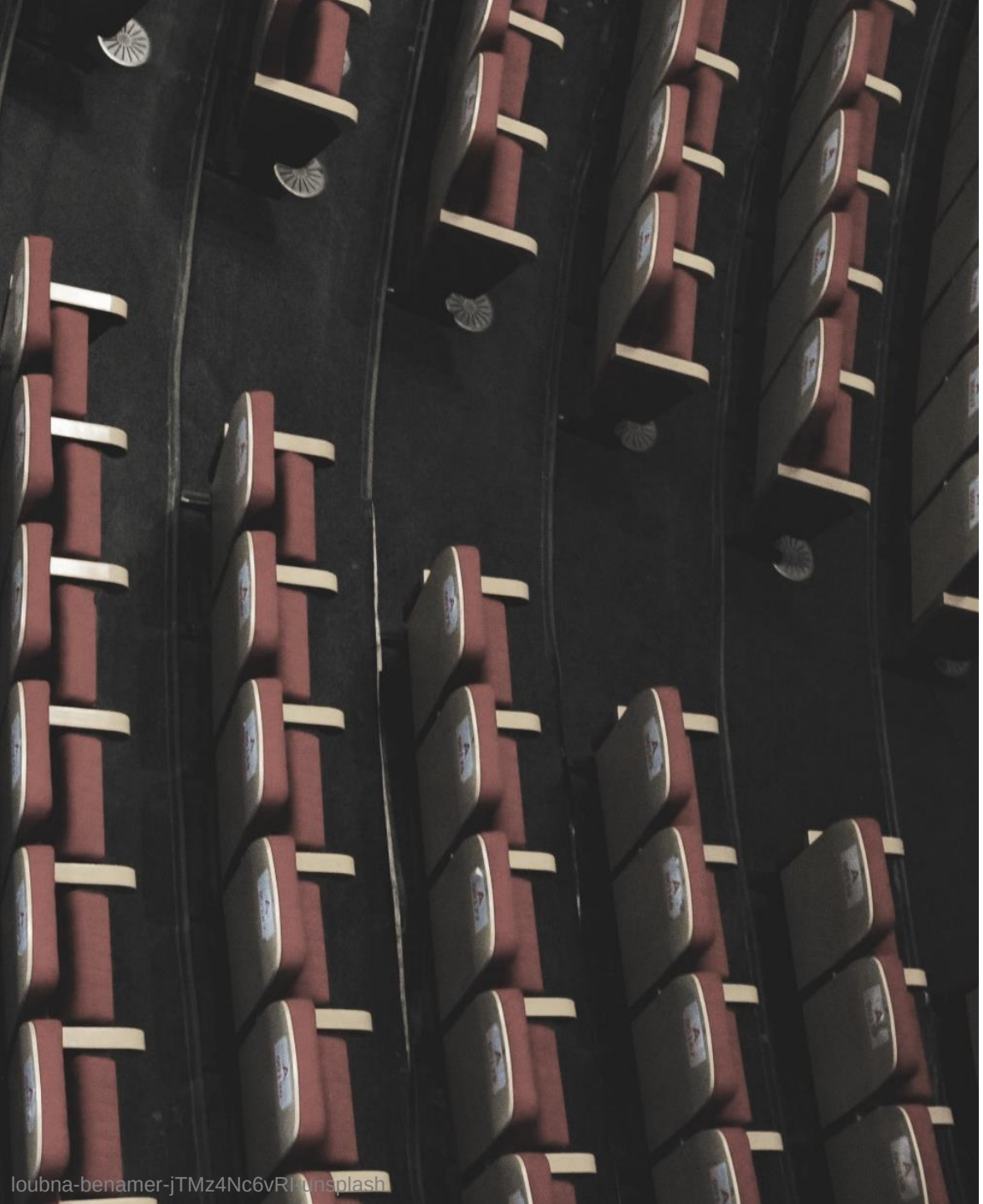
§ 7a BSIG

- **Untersuchungsrecht** des BSI hinsichtlich auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene IT-Produkte und –Systeme. Untersuchung durch Dritte möglich.
- **Auskunftspflicht** inkl. technischer Details („soweit erforderlich … alle notwendigen Auskünfte …“)
- **Informationsweitergabe** des BSI an Aufsichtsbehörde des Bundes oder an Ressort, wenn Behörde nicht vorhanden.
- BSI kann Erkenntnisse **weitergeben** und **veröffentlichen**, soweit erforderlich nach § 3 Abs. 1 S. 2 Nr. 1, 14, 14a, 17, 18 BSIG. Zuvor ist dem Hersteller Gelegenheit zur Stellungnahme zu geben.
- BSI kann **Öffentlichkeit** namentlich (Hersteller, Produkt) **informieren**, wenn Auskunft unterlassen wird und Gelegenheit zur Stellungnahme gegeben wurde.

Weitergabe von Erkenntnissen, wenn erforderlich nach § 3 Abs. 1 S. 2 Nr. 1, 14, 14a, 17, 18 BSIG

HK2 Rechtsanwälte

- *Nr. 1: Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;*
- *Nr. 14: Beratung, **Information und Warnung** der Stellen des Bundes, der Länder sowie **der Hersteller, Vertreiber und Anwender** in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;*
- *Nr. 14a: Verbraucherschutz und **Verbraucherinformation** im Bereich der Sicherheit in der Informationstechnik, insbesondere **durch Beratung und Warnung** von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;*
- *Nr. 17: **Aufgaben** nach den §§ 8a bis 8c und 8f **als zentrale Stelle für** die Sicherheit in der Informationstechnik **Kritischer Infrastrukturen**, **digitaler Dienste** und **der Unternehmen im besonderen öffentlichen Interesse**;*
- *Nr. 18: Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a; [→ Aufgaben/ Befugnisse der nationalen Behörden für Cybersicherheitszertifizierung]*



loubna-benamer-jTMz4Nc6vRI-unsplash

HK2
Rechtsanwälte

Unternehmen im besonderen öffentlichen Interesse


Panumas nikhomkhai/Pexel.com

HK2 Rechtsanwälte

UBI (ohne Störfall-UBI)

- im Sinne von § 2 Abs. 14 Nr. 1 BSIG i.V.m. § 60 Abs. 1 Nr. 1 AWV: **Rüstungsunternehmen**
- **IT-Sicherheitsunternehmen für Verschlusssachen**, § 2 Abs. 14 Nr. 1 BSIG i.V.m. § 60 Abs. 1 Nr. 3 AWV)
- **Großunternehmen** und **USP-Unternehmen** nach § 2 Abs. 14 Nr. 2 BSIG

Für UBI nach § 2 Abs. 14 Nr. 1, 2 BSIG gilt:

§ 8f BSIG

- Abs. 1: **Selbsterklärung zur IT-Sicherheit** beim Bundesamt vorzulegen
  - Ziff. 1 welche **Zertifizierungen** im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,
  - Ziff. 2 welche sonstigen **Sicherheitsaudits** oder **Prüfungen** im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder
  - Ziff. 3 wie sichergestellt wird, dass die für das Unternehmen **besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden**, und **ob dabei der Stand der Technik eingehalten** wird.
- Abs. 5: **Pflicht zur Registrierung** und Einrichtung **Kontaktstelle**
- Abs. 7: Pflicht zur **Meldung von Störungen**
- Abs. 9: bei Verdacht eines Verstoßes gegen Abs. 5: BSI ggü. Wertschöpfung darlegen und Bestätigung eines WP beibringen, dass Unternehmen nach der RV kein UBI ist.

Untersagungsbefugbnisse bei mangelnder Vertrauenswürdigkeit (§ 9b Abs. 5 BSIG)

HK2 Rechtsanwälte

→ **Vertragliche Verpflichtungen und Rechtsfolgenverknüpfung**

1. **Pflichtenverstoß gegen die Garantieerklärung**
2. Angabe von **unwahren Tatsachenbehauptungen** in der Garantieerklärung
3. **Mangelnde Unterstützung** von Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung („erforderlicher Umfang in angemessener Weise“?)
4. Schwachstellen oder Manipulationen werden nicht unverzüglich, nachdem er davon Kenntnis erlangt, **beseitigt** und dem Betreiber der Kritischen Infrastruktur **gemeldet**.
5. Die kritische Komponente auf Grund von **Mängeln** ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.
6. Die kritische Komponente über **technische Eigenschaften** verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

louis-hansel-7RtM37cLJ3c-unsplash

HK2
Rechtsanwälte

Schaffung/ Begrenzung/ Konkretisierung vertraglicher **Ansprüche** gegen Hersteller/ Zulieferer

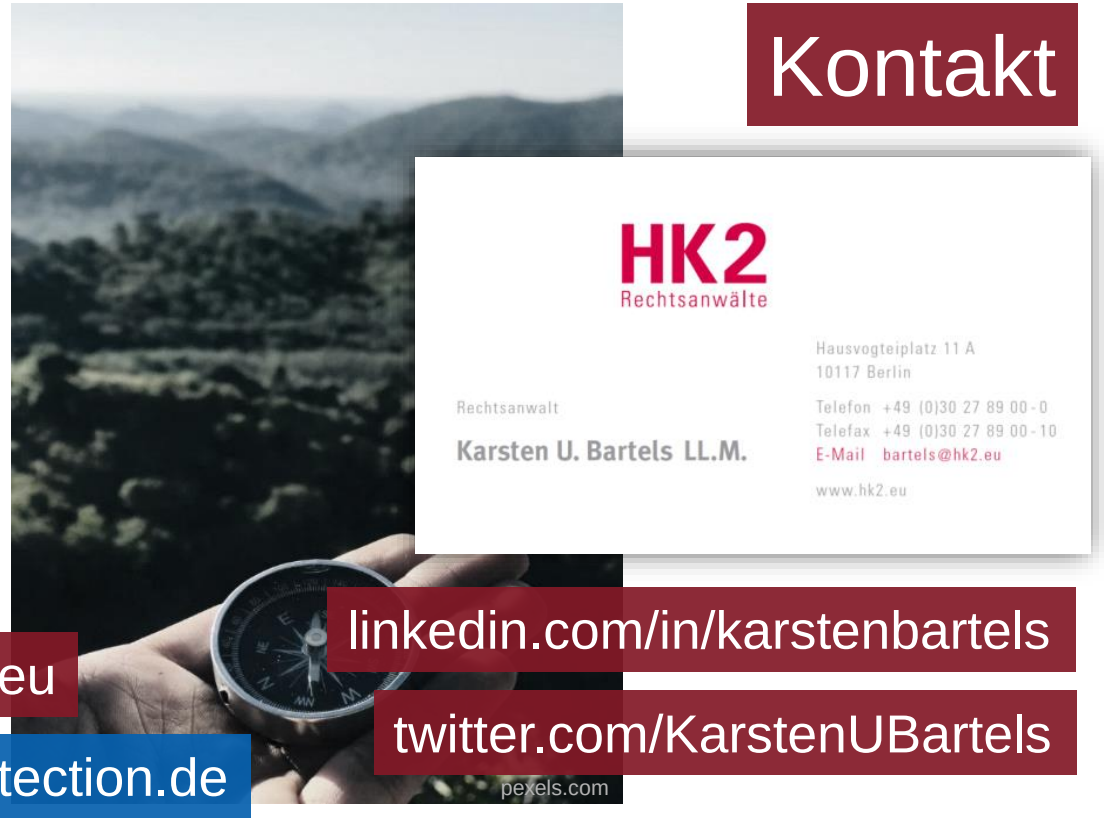
Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e.V.
- Lehrbeauftragter Hochschule Hof für Datenschutz-Compliance
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik

HK2
Rechtsanwälte

Kontakt



www.hk2.eu

www.comtection.de

linkedin.com/in/karstenbartels

twitter.com/KarstenUBartels