T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

NIS2-Umsetzungsgesetz

Aktueller Stand

RA Karsten U. Bartels LL.M.
HK2 Rechtsanwälte
Vorstand TeleTrusT, Leiter AG Recht

HK2
Rechtsanwälte

Karsten U. Bartels LL.M.*

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

*Rechtsinformatik

HK2

IT- und Datenrecht
Technik-Recht

IT-Sicherheitsrecht
Datenschutzrecht

Anwalt des Jahres für
Datenschutzrecht, Berlin 2023
Handelsblatt/ best lawyers

Karsten U. Bartels LL.M.

Liste der besten Anwälte
Deutschlands 2023
Handelsblatt/ best lawyers

Karsten U. Bartels LL.M.,
Dr. Jonas Jacobsen,
Bernhard Kloos,
Philip Koch

HK2 TOP-
Wirtschaftskanzlei 2023 für
IT & TK

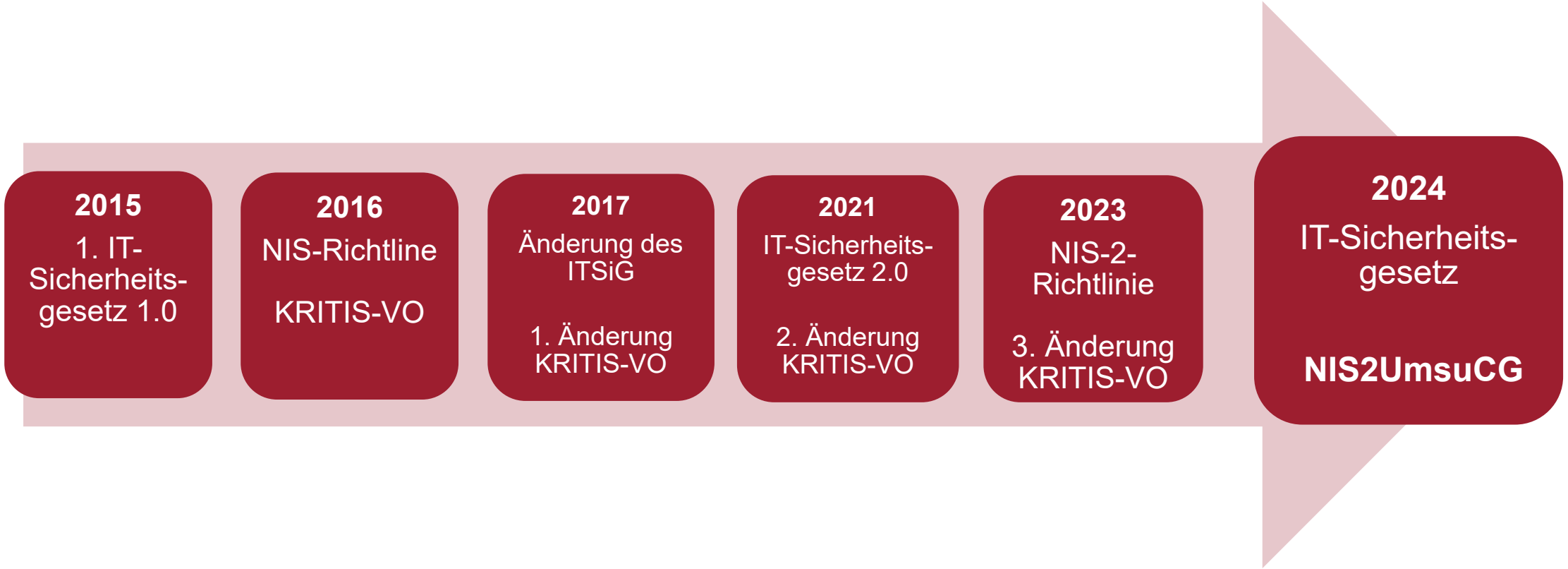
FOCUS BUSINESS 06/2023

NIS2-Umsetzungsgesetz

- Gesetzgebungsstand NIS2UmsuCG
- Systematische Änderungen und Anwendbarkeit
- Pflichten zur IT-Sicherheit
- Stand der Technik
- Weitere Pflichten wie Melde- und Registrierungspflicht
- Haftung der Geschäftsleitung
- Informationsaustausch mit dem BSI
- Warnungen des BSI
- Vorbereitung auf das NIS2UmsuCG

HK2 Rechtsanwälte

Entwicklung des IT-Sicherheitsgesetzes



HK2 Rechtsanwälte

Gesetzgebungsstand NIS2UmsuCG

2024

IT-Sicherheits-gesetz

NIS2UmsuCG

- Erster Referentenentwurf zum NIS2UmsuCG 03.04.2023
- Zweiter Referentenentwurf vom 03.07.2023
- Diskussionspapier vom 27.09.2023
  - Vorschriften zum BSI ausgenommen
  - Problem Ressortabstimmung
  - „Werkstattgespräch“ des BMI am 26.10.2023
  - BSI-Verordnung
  - Verbändebeteiligung zum NIS2UmsuCG-E
- geplante Verkündung Ende Q 1/ 2024
- Umsetzungsfrist

Artikel 41

Umsetzung

(1) Bis zum 17. Oktober 2024 erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Vorschriften ab dem 18. Oktober 2024 an.

(2) Bei Erlass der in Absatz 1 genannten Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

HK2
Rechtsanwälte

Artikel 29

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich der Absätze 2 und 3 am 1. Oktober 2024 in Kraft. Gleichzeitig tritt das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) außer Kraft.

(2) Artikel 2 tritt an dem Tag in Kraft, an dem [*die KRITIS-Dachgesetz-Verordnung*] in Kraft tritt, aber nicht vor dem Inkrafttretenstermin nach Absatz 1. Das Bundesministerium des Innern und für Heimat gibt den Tag des Inkrafttretens nach diesem Absatz im Bundesgesetzblatt bekannt.

(3) Artikel 27 tritt am 18. Oktober 2024 in Kraft.

Grundlegende Änderungen

- ca. 29.000 betroffene Unternehmen
- Neue Strukturierung des Anwendungsbereiches
  - Betreiber kritischer Anlagen
  - Besonders wichtige Einrichtungen
  - Wichtige Einrichtungen
- Aufnahme zusätzlicher Sektoren
- Ausweitung und Konkretisierung der Pflichten für Unternehmen
- Ausweitung Befugnisse des BSI
- Erweiterte Sanktionsvorschriften
- Pflichten für Einrichtungen der Bundesverwaltung

HK2 Rechtsanwälte

Einrichtungen der Bundesverwaltung

Erstmalige Aufnahme in den Anwendungsbereich des BSIG

- Stellen der Bundes
- Körperschaften, Anstalten und Stiftungen des Öff. Rechts und ihre Vereinigungen auf Bundesebene
- Mehrheitlich in Bundeseigentum stehende öffentliche Unternehmen, die für die Bundesverwaltung IT-Dienstleistungen erbringen

Von A.Savin - Eigenes Werk, FAL, https://commons.wikimedia.org/w/index.php?curid=81686930

HK2
Rechtsanwälte

… Verpflichtung der Länder und Kommunen?

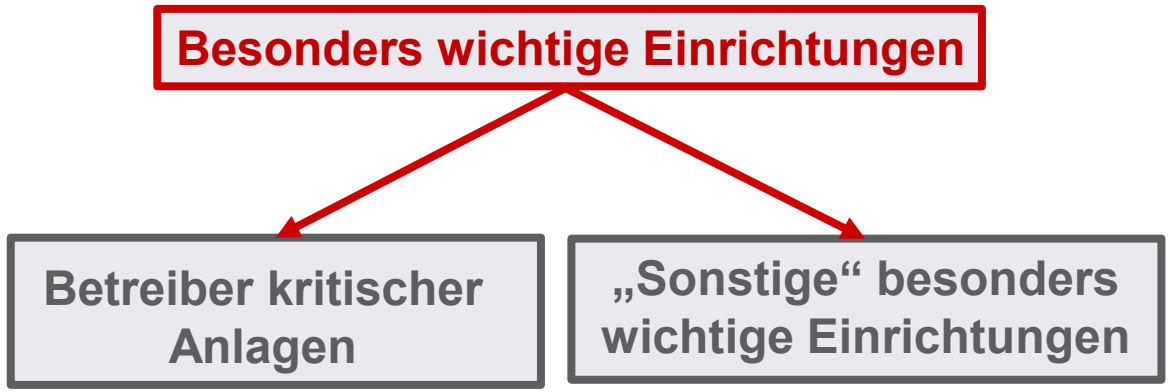
Von A.Savin - Eigenes Werk, FAL, https://commons.wikimedia.org/w/index.php?curid=81686930

HK2
Rechtsanwälte

Besonders wichtige Einrichtungen

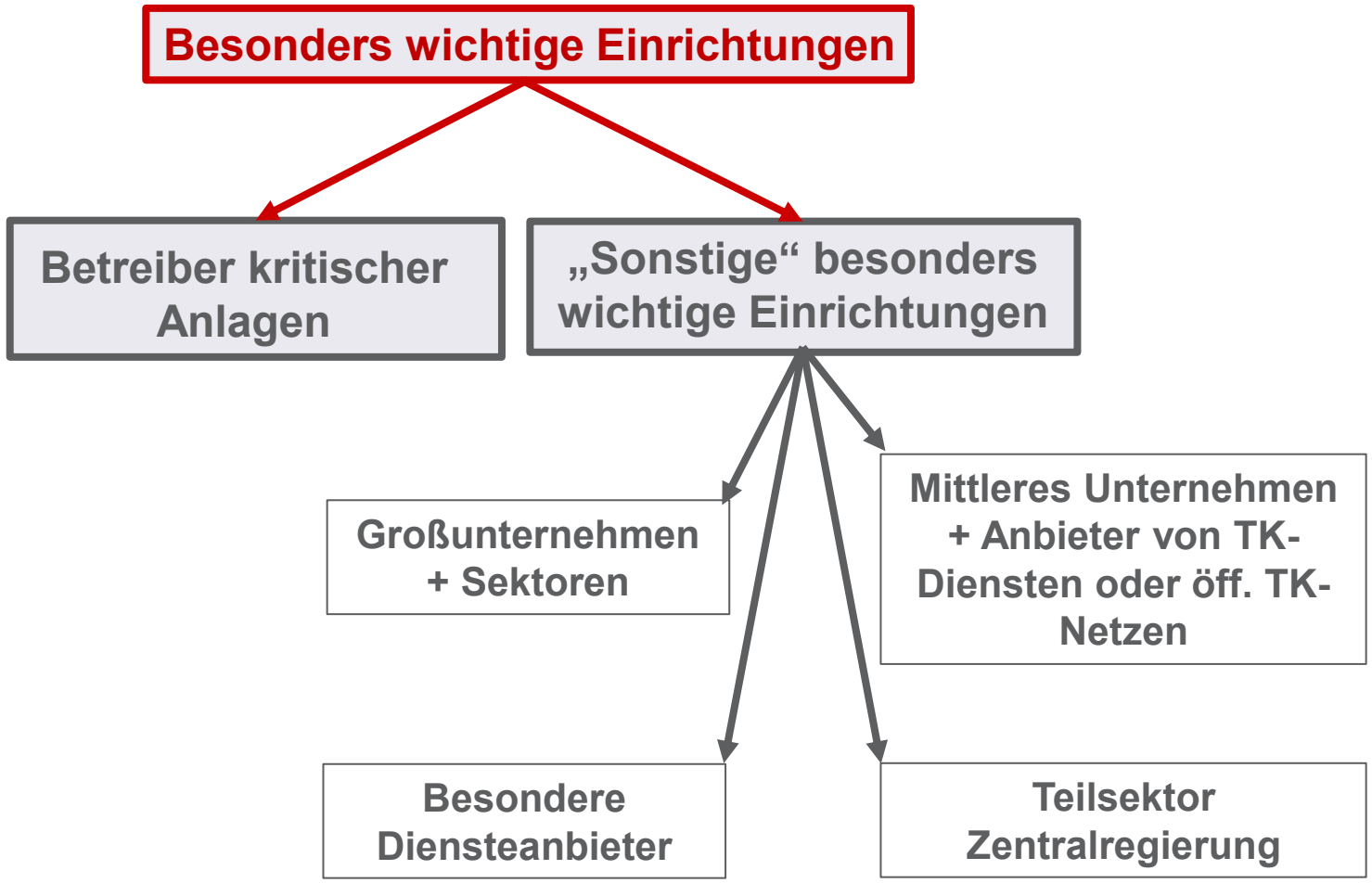
Wichtige Einrichtungen

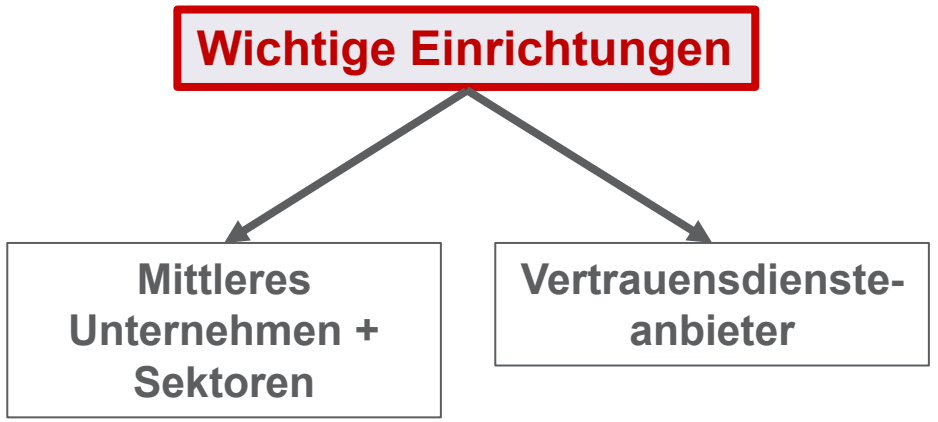
HK2
Rechtsanwälte



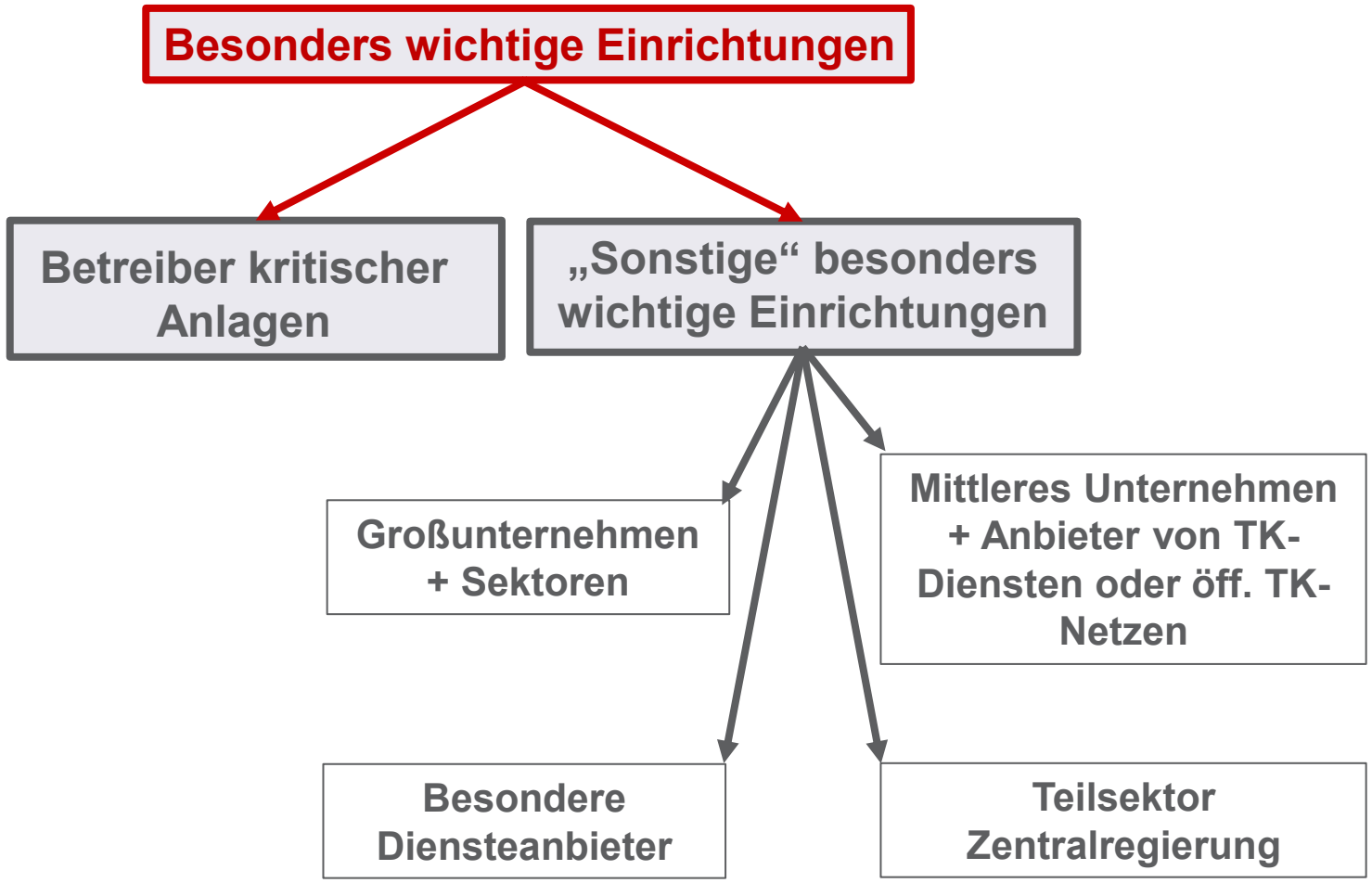
Wichtige Einrichtungen

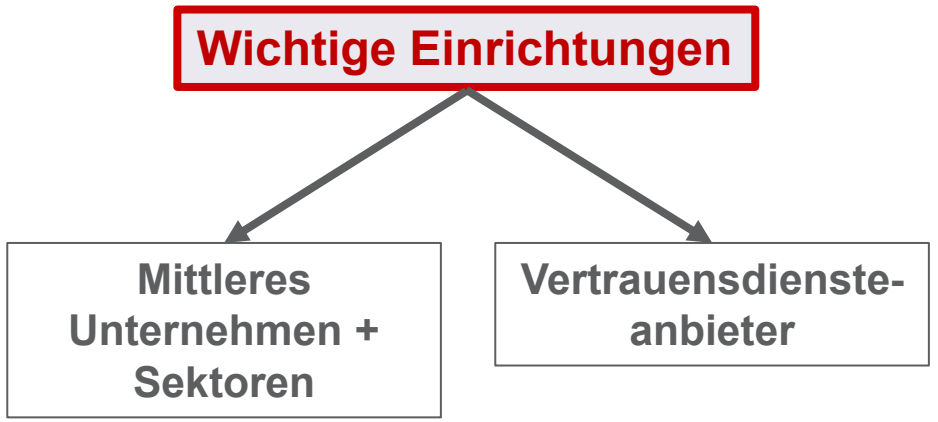
HK2 Rechtsanwälte





HK2 Rechtsanwälte





→ Einrichtungsarten der verschiedenen Sektoren jetzt in **Anlagen 1 und 2.** Zudem **Rechtsverordnung** gem. § 57 Abs. 1 BSIG-E

„Besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ gemäß § 28 Abs. 1 Ziff. 1 und Abs. 2 Ziff. 1

- erfasste Unternehmen
  1. natürliche oder juristische Personen oder rechtlich unselbständige Organisationseinheiten von Gebietskörperschaften, die
  2. anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet,
  3. die einer Einrichtungsart eines bestimmten Sektors zuzuordnen ist (vgl. Anlage 1 und 2) **und**
  4. eine bestimmte Größe aufweist.

- *Ref-E von 07/2023 enthielt noch „Großunternehmen“ und „Mittleres Unternehmen“ als Kernbegriffe*

HK2 Rechtsanwälte

Unternehmensgrößen im BSIG-E

Großunternehmen,
§ 28 Abs. 1 BSIG-E

250+ oder

und

50+ Mio. **43+ Mio.**

HK2 Rechtsanwälte

Unternehmensgrößen im BSIG-E

Großunternehmen,
§ 28 Abs. 1 BSIG-E

250+ oder

und

50+ Mio. **43+ Mio.**

Mittlere Unternehmen,
§ 28 Abs. 2 BSIG-E

50+ oder

und

10+ Mio. **10+ Mio.**

HK2 Rechtsanwälte

Unternehmensgrößen im BSIG-E

Großunternehmen,
§ 28 Abs. 1 BSIG-E

Mittlere Unternehmen,
§ 28 Abs. 2 BSIG-E

Unternehmen jeder Größe

250+ oder

und

50+ Mio. **43+ Mio.**

50+ oder

und

10+ Mio. **10+ Mio.**

Besonders wichtige Einrichtungen

Grahame Jenkins/Unsplash.com

HK2 Rechtsanwälte

Betreiber kritischer Anlagen, § 28 V, VI, VII BSIG-E

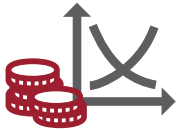
- Abs. 5: Ein **Betreiber kritischer Anlagen** ist…
  - eine natürliche oder juristische Person oder rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft,
  - die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss
  - auf eine kritische Anlage ausübt.
- Abs. 6: Eine **kritische Anlage** ist…
  - eine Anlage, die einem benannten Sektor zugehörig ist
  - und die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist.
  - Wird durch **Rechtsverordnung** nach § 57 Abs. 4 BSIG-E konkretisiert
    - → Anlage muss die dort festgelegten Schwellenwerte erreichen oder überschreiten (wie zuvor)
- Abs. 7: eine Anlage ist …
  - kritische Anlage, wenn Anlagenart der VO zuzuordnen ist und Schwellenwert erreicht oder überschreitet.

HK2 Rechtsanwälte

Betreiber kritischer Anlagen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum


Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung


Trinkwasser


IT und TK


Transport und Verkehr


TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Abwasser


Gesundheit


Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel


Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen, § 28 I BSIG-E

Neben Betreibern kritischer Anlagen sind „sonstige“ besonders wichtige Einrichtungen:

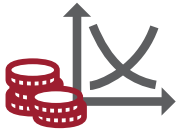
- **Großunternehmen**, das einer Einrichtungsart eines relevanten Sektors zuzuordnen ist (i. V. m. Anlage 1)
- **Qualifizierter Vertrauensdiensteanbieter**, **TLD Name Registries** oder **DNS-Diensteanbieter** (unabhängig von Unternehmensgröße)
- **Mittleres Unternehmen,** das Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen ist
- Einrichtungen des Teilsektors **Zentralregierung** des Sektors öffentliche Verwaltung

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Großunternehmen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum


Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung


Trinkwasser


IT und TK


Transport und Verkehr

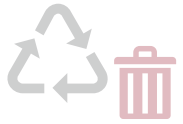

TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Abwasser


Gesundheit


Siedlungsabfall-entsorgung


Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

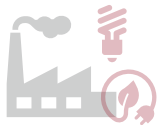
DNS-Diensteanb.

Lebensmittel

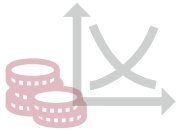

Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Mittlere Unternehmen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum

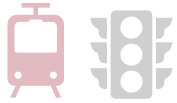

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung

Trinkwasser

IT und TK


Transport und Verkehr

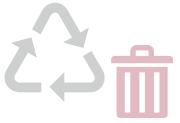

TLD Name Registries


Chemie

Verarbeitendes Gewerbe

Abwasser


Gesundheit


Siedlungsabfall-entsorgung


Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel


Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Unternehmen jeder Größe

Energie

Ernährung

Finanz- u. Versicherungsw.

Weltraum

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)

Forschung

Trinkwasser

IT und TK

Transport und Verkehr

TLD Name Registries

Chemie

Verarbeitendes Gewerbe

Abwasser

Gesundheit

Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel

Anb. digitaler Dienste

Wichtige Einrichtungen

HK2 Rechtsanwälte

Wichtige Einrichtungen, § 28 II BSIG-E

- **Mittleres Unternehmen,** das einer Einrichtungsart eines relevanten Sektors zuzuordnen ist (i. V. m. Anlagen 1 und 2)

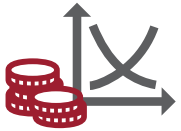
- **Vertrauensdiensteanbieter**

HK2 Rechtsanwälte

Wichtige Einrichtungen – Mittlere Unternehmen


Energie


Ernährung


Finanz- u. Versicherungsw.


Weltraum


Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)


Forschung


Trinkwasser


IT und TK


Transport und Verkehr


TLD Name Registries


Chemie


Verarbeitendes Gewerbe


Abwasser


Gesundheit


Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.


Lebensmittel


Anb. digitaler Dienste

HK2 Rechtsanwälte

Wichtige Einrichtungen – Unternehmen jeder Größe

Energie

Ernährung

Finanz- u. Versicherungsw.

Weltraum

Vertr.diensteanb (qual./normal)

Öff. Verwaltung (Zentralreg.)

Forschung

Trinkwasser

IT und TK

Transport und Verkehr

TLD Name Registries

Chemie

Verarbeitendes Gewerbe

Abwasser

Gesundheit

Siedlungsabfall-entsorgung

Anb. von TK-Diensten o. öff. zugänglichen TK-Netzen

DNS-Diensteanb.

Lebensmittel

Anb. digitaler Dienste

HK2
Rechtsanwälte

Pflichten für Betroffene, §§ 30 ff. BSIG-E

- Risikomanagementmaßnahmen
- Meldepflichten
- Registrierungspflicht
- Unterrichtungspflicht
- Billigungs-, Überwachungs- und Schulungspflicht
- Nachweispflichten für KRITIS-Betreiber
- Besondere Pflichten für Einrichtungen der Bundesverwaltung
- und mehr…

Nachweispflichten für KRITIS-Betreiber, § 39 BSIG-E

- Nachweis der Erfüllung der Anforderungen nach §§ 30 Abs. 1, 31 BSIG-E
  - Anders als im Ref-E nun im Diskussionspapier: **nur für KRITIS-Betreiber!**
- Frühestens drei Jahre nach Inkrafttreten des Gesetzes, anschließend alle drei Jahre
  - *Fristen sollen für auch für wE und bwE gelten (für welche Pflichten?)*
- Kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen
- Übermittlung an BSI, ggf. Nachweis auch über die Beseitigung aufgetretener Mängel

Aber: § 64 III (Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen):

„Das Bundesamt kann von besonders wichtigen Einrichtungen Nachweise über die Erfüllung einzelner oder aller Anforderungen nach den §§ 30, 31 und 32 verlangen“

Risikomanagementmaßnahmen für besonders wichtige und wichtige Einrichtungen, § 30 BSIG-E

HK2 Rechtsanwälte

- Abs. 1: geeignete, verhältnismäßige und wirksame **technische und organisatorische Maßnahmen**
  - Risikoexposition, Größe Einrichtung/ Betreiber, Risiko (Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen, gesellschaftliche Auswirkungen) und Umsetzungskosten zu berücksichtigen.
- Abs. 2: Maßnahmen
  - sollen **Stand der Technik** einhalten
  - **Normen** berücksichtigen und
  - müssen auf „gefahrenübergreifendem Ansatz beruhen“
  - Katalog mit **Mindestanforderungen** z. B. Risikoanalysekonzepte, Lieferkettensicherheit, Cyberhygiene, Verschlüsselung u. v. m.
- bleibt möglich: Branchenspezifische Sicherheitsstandards (B3S), Abs. 9

Technische und organisatorische Maßnahme Mindestanforderungen,§ 30 IV BSIG-E

HK2 Rechtsanwälte

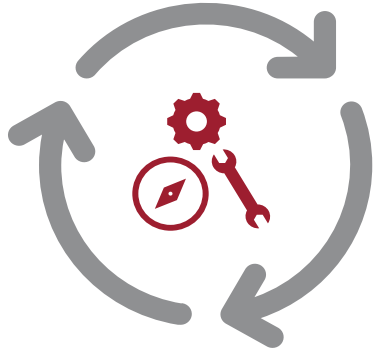
1. **Konzepte** in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von **Sicherheitsvorfällen**
3. **Aufrechterhaltung** des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der **Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
5. **Sicherheitsmaßnahmen** bei **Erwerb**, **Entwicklung** und **Wartung** von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich **Management und Offenlegung von Schwachstellen**

Technische und organisatorische Maßnahme Mindestanforderungen,§ 30 IV BSIG-E

6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von **Kryptografie** und **Verschlüsselung**
9. Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle** und **Management von Anlagen**
10. Verwendung von Lösungen zur Multi-Faktor-**Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte **Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte **Notfallkommunikationssysteme** innerhalb der Einrichtung.

Technische und organisatorische Maßnahmen
§ 30 Abs. 2

*„(2) Maßnahmen nach Absatz 1 sollen den **Stand der Technik** einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen: …“*



Stand der Technik

HK2
Rechtsanwälte

Zu beobachten :/

(4) Soweit die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen festgelegt werden, so gehen diese den in Absatz 2 genannten Maßnahmen vor.

(5) Soweit die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.

Besondere Anforderungen an die Risikomanagementmaßnahmen von KRITIS-Betreibern, § 31 BSIG-E

HK2 Rechtsanwälte

- Abs. 1: für IT-Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der kritischen Anlage maßgeblich sind, gelten **auch aufwändigere Maßnahmen als verhältnismäßig**!
  - Erforderlicher Aufwand darf dennoch nicht außer Verhältnis zu Folgen von Beeinträchtigung/Ausfall stehen

- Abs. 2: Erforderlichkeit von **Systemen zur Angriffserkennung**

Besondere Pflichten für Betreiber kritischer Anlagen §§ 39, 41 BSIG-E

- Systeme zur Angriffserkennung, § 39 BSIG-E
  - definiert in § 2 Abs. 1 Nr. 38 BSIG-E
  - Identifizierung von Bedrohungen
  - Stand der Technik, aber verhältnismäßiger Aufwand
  - Auch Teil der Nachweispflicht nach § 34 BSIG-E

- Einsatz kritischer Komponenten, § 41 BSIG-E
  - definiert in § 2 Abs. 1 Nr. 20 BSIG-E
  - Anzeigepflicht an BSI vor Einsatz der Komponente
  - Untersagung durch BSI innerhalb von 2 Monaten möglich
  - Einsatz nur bei Erklärung über Vertrauenswürdigkeit durch Hersteller der Komponente (Garantieerklärung)

HK2 Rechtsanwälte

Meldepflichten, § 32 BSIG-E

- Betrifft **besonders wichtige und wichtige Einrichtungen**
- Meldepflicht an BSI bei **erheblichen Sicherheitsvorfällen**
  - Sicherheitsvorfall, § 2 Abs. 1 Nr. 35 BSIG-E
  - Erheblicher Sicherheitsvorfall, § 2 Abs. 1 Nr. 9 BSIG-E
- Mehrstufiges Meldeverfahren in Abs. 1 (s. sogleich)
- Zusätzliche Meldepflicht für KRITIS-Betreiber in Abs. 3

- *Meldemöglichkeiten sollen vollumfänglich digital gestaltet werden.*
- *Kommunikation: Deutsch ist Amtssprache, Englisch aber teilw. möglich*

HK2 Rechtsanwälte

Meldepflichten, § 32 BSIG-E

Stufe 1: frühe Erstmeldung, Nr. 1	• **24 h; Vorfall wegen rechtswidriger/böswilliger Handlungen? Grenzüberschreitende Auswirkungen?**
Stufe 2: bestätigende Erstmeldung, Nr. 2	• **72 h; Bestätigung der Informationen; erste Bewertung: Schweregrad? Auswirkungen? Kompromittierungsindikatoren?**
Stufe 3: Zwischenmeldung, Nr. 3	• **Statusaktualisierung auf Ersuchen des BSI**
Stufe 4: Abschlussmeldung, Nr. 4	• **1 Monat; ausführliche Beschreibung; Art und Ursache; Abhilfemaßnahmen; grenzüberschreitende Auswirkungen**

Abs. 2: ggf. statt Abschlussmeldung Fortschrittsbericht, wenn Vorfall noch andauert

HK2 Rechtsanwälte

Registrierungspflicht, § 33 f. BSIG-E

- Betrifft **besonders wichtige und wichtige Einrichtungen** sowie Domain-Name-Registry-Diensteanbieter
- Spätestens nach **3 Monaten** Registrierung beim BSI
- Für **KRITIS-Betreiber:** Erweiterung der Registrierungspflicht auch auf die kritischen Anlagen
- § 34: Besondere Registrierungspflichten für in § 63 BSIG-E genannte Einrichtungen (§ 63 fehlt im Diskussionspapier) bis zum 17.01.2025. Im Entwurf 07/2023 waren dies:
  - Cloud Computing-Dienste, Anbieter von Rechenzentrumsdiensten
  - Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider
  - Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke
- Bei Nichteinhaltung: Registrierung durch BSI selbst, § 33 Abs. 3 BSIG-E

- *Pflichten sollen erst gelten, wenn gelten, wenn Melde und Registrierungsmöglichkeiten vorhanden sind.*

HK2 Rechtsanwälte

Weitere Pflichten

- Unterrichtungspflichten, § 35 BSIG-E
  - Bes. wichtige und wichtige Einrichtungen haben auf Anweisung des BSI die Empfänger ihrer Dienste bzgl. Sicherheitsvorfällen zu unterrichten
- Billigungs-, Überwachungs- und Schulungspflicht für Leitungsorgane, § 38 BSIG-E
  - Geschäftsleiter haben die TOM zu billigen und ihre Umsetzung zu überwachen
  - Geschäftsleiter haben regelmäßig an Schulungen teilzunehmen
- Pflichten für TLD Name Registries und Domain-Name-Dienstleister, § 51 BSIG-E

moerschy/Pixabay.com

HK2
Rechtsanwälte

Persönliche Haftung der Geschäftsleitung

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.

(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Satz 1 gilt nicht für Geschäftsleiter besonders wichtiger Einrichtungen des Teilsektors Zentralregierung des Sektors öffentliche Verwaltung.

(3) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wer tige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrer bigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan ger

(4) Die Geschäftsleiter von besonders wichtigen Einrichtungen und tungen müssen und deren Mitarbeiter sollen regelmäßig an Schulunge ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertu wie Risikomanagementpraktiken im Bereich der Cybersicherheit und de auf die von der Einrichtung erbrachten Dienste zu erwerben.

HK2 Rechtsanwälte

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

(2) Ein Verzicht der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten nach Absatz 1 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(3) Die Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

HK2 Rechtsanwälte

Haftung der Geschäftsleitung

§ 64 Abs. 10 BSIG-E

Sofern besonders wichtige Einrichtungen den Anordnungen des BSI trotz Fristsetzung nicht nachkommen, kann das BSI die jeweils zuständige Aufsichtsbehörde des Bundes auffordern
1. die Genehmigung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung vorübergehend auszusetzen

*2. **den natürlichen Personen**, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in der besonders wichtigen Einrichtung zuständig sind, die Wahrnehmung der **Leitungsaufgaben vorübergehend untersagen**.*

Pflicht zur Legalität bedingt die Einrichtung eines Compliance Management Systems

OLG Nürnberg, Endurteil v. 30.03.2022 – 12 U 1520/19

Titel:

Haftung des Geschäftsführers einer GmbH & Co KG für Pflichtverletzungen im Rahmen der internen Unternehmensorganisation

Normenketten:

GmbHG § 43 Abs. 1, Abs. 2, § 46 Nr. 8
AktG § 93 Abs. 1 S. 2, Abs. 2 S. 2, § 147 Abs. 2
HGB § 146 Abs. 1

Leitsätze:

1. Der Geschäftsführer einer GmbH, deren wesentliche Aufgabe in der Führung der Geschäfte einer Kommanditgesellschaft besteht, haftet (auch) dieser KG gegenüber gemäß § 43 Abs. 2 GmbHG. (Rn. 70)
2. Zum Umfang der Pflichten eines Geschäftsführers im Rahmen der internen Unternehmensorganisation (hier: Schaffung von Compliance-Strukturen zur gehörigen Überwachung von Mitarbeitern). (Rn. 102 – 108)
3. Unterlässt der Geschäftsführer eine Unternehmensorganisation, die die Wahrung des Vier-Augen-Prinzips für schadensträchtige Tätigkeiten erfordert, so kann er für hierdurch entstehende Schäden haften. (Rn. 137)

OLG Nürnberg (12 U 1520/19)

moerschy/Pixabay.com

HK2 Rechtsanwälte

Sanktionen, § 60 BSIG-E

- Bußgelder von EUR 100.000 bis 2 Mio.
- Für wichtige Einrichtungen: EUR 100.000 bis 7 Mio. bzw. 1,4 % des weltweiten Umsatzes
- Für besonders wichtige Einrichtungen (inkl. Betreiber kritischer Anlagen): EUR 100.000 bis 10 Mio. bzw. 2 % des weltweiten Umsatzes

HK2 Rechtsanwälte

Informationsaustausch, § 6

„(1) Das Bundesamt ermöglicht den Informationsaustausch besonders wichtiger Einrichtungen und wichtiger Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern untereinander zu Cyberbedrohungen, Beinahevorfällen, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen. Es betreibt dazu ein geeignetes ***Online-Portal****.*

(2) Die Teilnahme am Informationsaustausch steht ***grundsätzlich*** *allen besonders wichtigen* ***Einrichtungen****, wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen* ***Lieferanten oder Dienstleistern*** *offen. Das Bundesamt kann entsprechende* ***Teilnahmebedingungen*** *erstellen, die die Teilnahme am Informationsaustausch regeln. Das Bundesamt* ***kann*** *weiteren Stellen die Teilnahme* ***ermöglichen*** *“*

Warnungen, § 13 BSIG-E (07/2023)

§ 7 BSIG

- Warnungen/ Infos an die Öffentlichkeit o. betroffene Kreise (Abs. 1)
  - a) Warnungen vor **Sicherheitslücken** in IT-Produkten und Diensten
  - …

Neu: § 13 BSIG-E

- Warnungen/ Infos an die Öffentlichkeit o. betroffene Kreise (Abs. 1)
  - a) Warnungen vor **Schwachstellen und anderen Sicherheitsrisiken** in IT-Produkten und Diensten
  - …
  - e) Informationen über **Verstöße** besonders wichtiger oder wichtiger Einrichtungen **gg. Pflichten aus diesem Gesetz** [und anderen Gesetzen, die die NIS-2-RL umsetzen]

Warnungen signifikant häufiger möglich!

- Sicherheitslücke = Schwachstelle
- Sicherheitsrisiko? Nicht definiert. BSI legt fest?
- Jeder Verstoß gegen das BSIG-E (und andere Umsetzungsgesetze) begründet das Recht des BSI eine Warnung an die Öffentlichkeit zu richten!

HK2 Rechtsanwälte

Was ist bereits jetzt zu tun?

- Vorab-Bestimmung: wäre mein Unternehmen im Anwendungsbereich?
- Geschäftsleitung und betroffene Abteilungen informieren und einbeziehen.
- IT-Sicherheitsstrategie und Budgets anpassen.
- Projektplan zur IT-Compliance erstellen/ anpassen.
- „Risikomanagementmaßnahmen“ gem. § 30 BSIG-E prüfen/ umsetzen/ anpassen.
- IT-Sicherheitsvereinbarungen mit Kunden vorbereiten! Kommunikation anpassen.
- IT-Sicherheit mit Zulieferern/ Dienstleistern nachverhandeln!

HK2 – Der Rote Faden

Sehr geehrter Herr Bartels,

meine Lieblings-Sentenz von Julian Nida-Rümelin ist: „Ich bin affizierbar durch Gründe." Gedankenpause. Wunderbar. Ich auch. Gründe muss man manchmal auch suchen. Das dachte sich wohl auch die Post, die jetzt tatsächlich eine „Briefankündigung im E-Mail Postfach" als neuen Service anbietet. Mir werden hier Scans der Umschläge der Briefe, die ich postalisch erhalte, vorab gemailt. Nur die Umschläge. Begründung: „Immer und überall informiert" zu sein. Andere digitalisieren die Welt, wir scannen Briefumschläge. Was für ein possierlicher Unfug.

Die Verlinkung zum Dienst habe ich nicht vergessen, aber ich kann Euch/ Ihnen auf Wunsch gern den Roten Faden ausgedruckt im Kuvert schicken und vorab das Bild vom Umschlag mailen. Vielleicht gibt's ja doch Gründe …

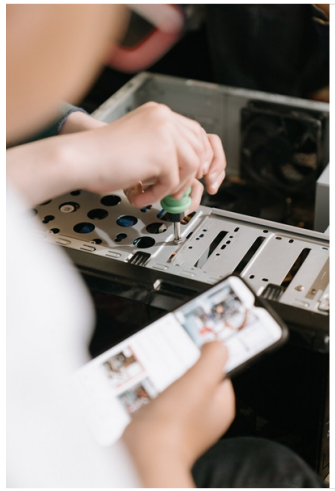
Nun denn - den Roten Faden spinnen wir in dieser Ausgabe unter anderem um die Fragen, wann eine rechtliche Information – zum Beispiel im Zusammenhang mit der Corona-Pandemie – unzulässig sein kann, wie unterschiedlich Gerichte Influencer-Marketing beurteilen und warum fehlende Querverweise in AGB womöglich taktisch gar nicht so hilfreich sind wie gedacht.

Viel Spaß bei der Lektüre

wünscht Euch/ Ihnen

Karsten U. Bartels

P.S.: meine besten Glückwünsche an Matthias und die weiteren HK2-AutorInnen zur Buchveröffentlichung, siehe unten!



Red Flags

Wiederverkauf nach Änderung der Firmware verboten

Wer etwa ein Auto kauft, darf es wieder verkaufen, auch wenn darauf die Marke des Herstellers angebracht ist. Dieses Verständnis dürfte den meisten so trivial erscheinen, dass sie darüber kaum je nachdenken. Bei Privatverkaufen ist das auch unproblematisch, weil das Markenrecht auf diese keine Anwendung findet. Im geschäftlichen Verkehr dagegen unterliegt dieser „**Erschöpfung**" genannte Grundsatz als Ausnahme vom Markenschutz Grenzen. Er gilt ggf. nicht für **Importwaren** aus Staaten außerhalb des EWR oder für **veränderte Produkte**. Und eine solche Veränderung liegt – so das LG München I (17 HK O 1703/20) – auch vor, wenn ein Händler die **abgespeckte Firmware** gebrauchter Router einer Sonderedition gegen die aktuelle, **funktionsreichere Firmware** des Router-Herstellers für die Standard-Geräte gleichen Typs austauscht. Dass dies zu einer **Verbesserung** führt oder, dass es sich um die **Original- Firmware des Herstellers** für diesen Router-Typ handelt, spielt dabei keine Rolle.

Philip Koch

Irreführung durch Kundeninformationen

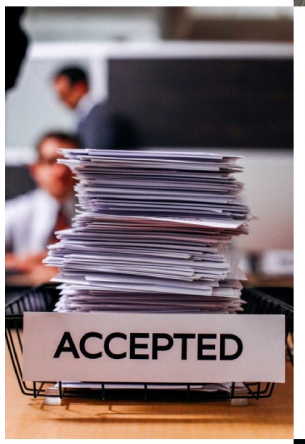
Ob Gutscheine statt Rückzahlung, abweichende Lieferbedingungen oder Informationen zur Umsatzsteuersenkung. **Unternehmen informieren ihre Kunden** über Corona bedingte Besonderheiten in der Vertragsbeziehung. Werden in Kundeninformationen **Rechtsansichten** geäußert, können sie **wettbewerbswidrig** sein. Unzulässig laut BGH (I ZR 85/19):

- Die Behauptung einer eindeutigen Rechtslage, die nicht besteht.
- Für den Kunden ist nicht erkennbar, dass es sich um eine Rechtsansicht handelt, sondern er versteht die Äußerung als Feststellung.
- Objektiv falsche Auskünfte auf eine ausdrückliche Nachfrage des Kunden.

Rechtsansichten sind als Meinungsäußerungen zulässig, wenn der Kunde sie als solche erkennen kann. **Es kommt also auf die ganz konkrete Formulierung an.**

Die Kommunikation mit dem Kunden bedarf daher immer einer rechtlichen Prüfung. Selbst bei der Formulierung von Zahlungsaufforderungen oder Kündigungsschreiben besteht das Risiko, die vom BGH aufgezeigten Grenzen des Zulässigen zu überschreiten.

Nadja Marquard



BGH zur AGB-Auslegung beim Verwenden mehrerer Klauselwerke

Es gibt Anbieter, die AGB als verwobene, epische Patchworks verstehen. Das geht leider schief.

So hatte der BGH (VIII ZR 289/19) kürzlich über die Wirksamkeit einer in AGB enthaltenen Inkassokostenpauschale zu entscheiden. Dabei hat er sich auch zur Auslegung von AGB beim **Verwenden mehrerer Klauselwerke** geäußert und eine Einbeziehung von separaten Urkunden, auf die in der jeweiligen Klausel nicht gesondert hingewiesen worden war, verneint.

Zwar seien bei der Auslegung einer AGB-Klausel grundsätzlich auch inhaltlich verbundene Bestimmungen eines „Gesamtklauselwerks" zu berücksichtigen. Dagegen seien aber Bestimmungen, die in **gesonderten Urkunden** niedergelegt sind und auf die die beanstandete Formularklausel nicht konkret Bezug nimmt, grundsätzlich nicht zur Auslegung dieser Klausel heranzuziehen. Dem Kunden kann insbesondere nicht abverlangt werden, **verschiedene Klauselwerke nach Anhaltspunkten zu durchforsten**, wie ein bestimmter Begriff noch weiter zu verstehen sein könnte.

Ronja Hecker

Influencer Chaos auch in den Berufungsinstanzen

Die Frage, ob ein Influencer auch **kommerzielle Posts ohne Gegenleistung** zu kennzeichnen hat, wird auch von den **Berufungsinstanzen unterschiedlich** gesehen.

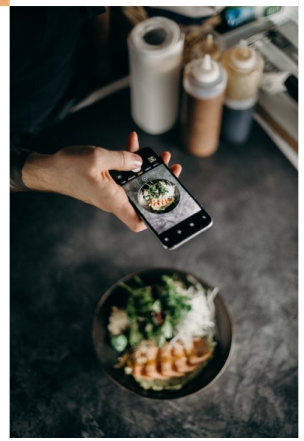
Schon das LG München (4 HK O 14312/18) hatte entschieden, dass im Fall prominenter Personen mit hoher Followerzahl für den **Nutzer offensichtlich** ist, dass **kommerzielle Interessen** verfolgt werden und Beiträge mangels Irreführung nicht zu kennzeichnen sind. Dieser Ansicht ist nun das OLG Hamburg (15 U 142/19) gefolgt.

Das OLG München (29 U 2333/19) geht noch einen Schritt weiter: Unentgeltliche Posts seien schon **keine kommerzielle Handlung**. Das allgemeine Interesse, sich durch Publikationen für Werbeverträge interessanter zu machen, genügt nicht. Die **Absatzförderung der Produkte** sei nur ein **zufälliger Reflex** eines ansonsten redaktionellen Handelns.

Das OLG Braunschweig, (2 U 78/19) und das OLG Frankfurt a.M. (6 W 68/19) haben das anders gesehen und gehen von einer **generellen Kennzeichnungspflicht** aus.

Wann und ob der **BGH die Gelegenheit** bekommt, diese Unstimmigkeit zu klären, ist noch ungewiss.

Sina Schmiedefeld



HK2 Insights

KI & Recht kompakt

Künstliche Intelligenz ist eine **Basistechnologie**, die in allen Bereichen des täglichen Lebens, in allen Produkten und in der Arbeitswelt eine Rolle spielen wird.

Die Auswirkungen dieser technologischen Revolution sind noch gar nicht absehbar.

Schon jetzt wirft KI in vielen Rechtsbereichen aber ganz praktische, **juristische Fragen** auf. Wir freuen uns - und sind auch ein wenig stolz - gemeinsam mit **exzellenten Autoren**, die sich mit KI bereits länger intensiv auseinandersetzen, in dem soeben bei Springer Vieweg erschienenen Buch **KI & Recht** zur Diskussion der Implikationen von KI in der Rechtspraxis beizutragen.

Das Buch behandelt die technischen Grundlagen und die Auswirkungen im Zivil-, Urheber-, Datenschutz-, Straf- und Arbeitsrecht.

Matthias Hartmann,
Jörg Hennig,
Bernhard Kloos und Anika Nadler

dunkelrot

Schluss mit den Geheimprozessen?

Das **Bundesverfassungsgericht** meint es ernst mit fairen Verfahren, auch im Wettbewerbsrecht. Es hat nun bestätigt, dass die für das **einstweilige Verfügungsverfahren** aufgestellten **Grundsätze zur prozessualen Waffengleichheit** (wie zu erwarten) auch im **Wettbewerbsrecht** gelten (1 BvR 1379/20).

Eilverfahren sind im gewerblichen Rechtsschutz und Äußerungsrecht besonders beliebt, um Unterlassungsansprüche schnell und effektiv durchzusetzen. Der Gegner wird wegen der vermeintlichen Dringlichkeit **in der Praxis in aller Regel nicht angehört**, obwohl die Nichtanhörung gesetzlich nur als Ausnahme festgelegt ist.

2018 **korrigierte** das Bundesverfassungsgericht die **praktische Umkehr des Regel- Ausnahmeverhältnis** in zwei Entscheidungen aus dem Presse- und Äußerungsrecht (BVerfG, 1 BvR 1783/17, II.2.a und 1 BvR 1783/17, II.2.b).

Wurde der Gegner nicht außergerichtlich abgemahnt oder weicht die Unterlassungserklärung aus der Abmahnung von dem bei Gericht geltend gemachten Unterlassungsantrag ab oder erteilt das Gericht dem Antragsteller richterliche Hinweise, muss das Gericht dem Gegner Gehör gewähren. Tut es das nicht, ist die prozessuale Waffengleichheit verletzt. Eine Ausnahme besteht nur in den seltenen Fällen der Beeinträchtigung des Rechtsschutzziels bei Anhörung (bspw. Sequestration).

Ob die Zivilgerichte diese Grundsätze auch tatsächlich umsetzen ist zweifelhaft. Sie wurden jedenfalls zwei Jahre nach den Entscheidungen in dem der Verfassungsbeschwerde zugrundeliegenden Sachverhalt missachtet, der kein Einzelfall sein dürfte.

Sina Schmiedefeld

Compliance & Data Protection

Die Kolumne der HK2 Comtection GmbH

Auch für Kreative: EDSA-Leitline zur Einwilligung

Bereits im Mai hat der **Europäische Datenschutzausschuss (EDSA)** eine aktualisierte **Leitlinie zur DSGVO konformen Einwilligung** veröffentlicht. Anlass für die Aktualisierung war u. a. das **Cookie-Urteil des EuGHs 2019** (wir berichteten). Dennoch geht der EDSA, entgegen der vielleicht geweckten Erwartung, gar nicht so ausführlich auf die Cookie-Einwilligung ein. Allein Beispiel 6a stellt klar, dass ein Cookie-Banner, das die Inhalte eine Webseite verdeckt und erst nach Einwilligung zugänglich macht, keine wirksame Einwilligung ermöglicht. Daneben enthält die Leitlinie zahlreiche weitere **Praxisbeispiele** für wirksame und unwirksame Einwilligungen inkl. einiger **kreativer Ansätze**, wie das Smartphone im Uhrzeigersinn zu drehen. Wer also mit **unkonventionellen Einwilligungstechniken** experimentieren will, dem sei diese EDSA-Leitlinie als Lektüre empfohlen.

Kein allgemeiner Anspruch auf Unterlassung rechtswidriger Datenverarbeitung

Bei mir um die Ecke gab es bis vor Kurzem ein Graffiti „Schlechtes Abschaffen". Der Ansatz finde ich eigentlich gut. Folgt man dem VG Regensburg ist das zumindest im Datenschutz in dieser Allgemeinheit leider nicht möglich. In Bezug auf die Klage eines Bürgers gegen die Videoüberwachung eines Parks urteilte das Gericht kürzlich, die DSGVO enthalte **keinen allgemeinen Anspruch auf Unterlassung**, schlechter", weil **rechtswidriger Datenverarbeitung**. Die DSGVO kenne eben nur **Rechte des Betroffenen** wie Löschung und Berichtigung. Diese könnten dann auch gerichtlich geltend gemacht werden. Ansonsten bleibe nur die Beschwerde bei der Aufsichtsbehörde. Da die DSGVO die Rechtsbehelfe abschließend regele, sei die allgemeine **Leistungsklage** auf Grundlage eines **zivilrechtlichen Unterlassungsanspruchs nicht statthaft**.

Lukas Wagner LL.M.
Datenschutzbeauftragter der HK2 Comtection GmbH

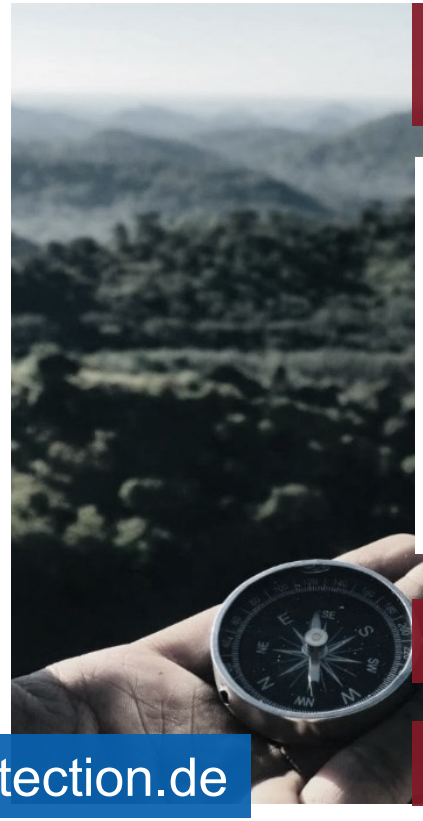
Michael Schramm LL.M. (Minnesota)
Datenschutzbeauftragter der HK2 Comtection GmbH

HK2 Rechtsanwälte

hk2.eu/newsletter

HK2
Rechtsanwälte

Slides + Kontakt



HK2
Rechtsanwälte

Hausvogteiplatz 11 A
10117 Berlin

Rechtsanwalt
Karsten U. Bartels LL.M.

Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
E-Mail bartels@hk2.eu

www.hk2.eu

www.hk2.eu

www.comtection.de

linkedin.com/in/karstenbartels