Rechtliche Aufgaben und Projektplanung zur NIS-2-Umsetzung.

RA Karsten U. Bartels LL.M.

16.05.2024, it-sa365

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Lehrbeauftragter für IT-Sicherheitsrecht, Ludwig-Maximilians-Universität München
- Vorsitzender Arbeitsgemeinschaft IT-Recht (davit) im Deutschen Anwaltverein
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit (TeleTrusT)
- Leiter AG IT-Sicherheitsrecht Bundesverband IT-Sicherheit (TeleTrusT)
- 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

Stand des Gesetzgebungsverfahrens

Leaks

- Leak Referentenentwurf vom 03.04.2023
- Leak Referentenentwurf vom 03.07.2023
- BMI: Diskussionspapier vom 27.09.2023 und „Werkstattgespräch“ am 26.10.2023
- Leak Referentenentwurf vom 22.12.2023 in 03/2024

Verbändebeteiligung durch BMI

- **Referentenentwurf vom 07.05.2024**
- **Stellungnahmen bis zum 28.05.2024**
- **Anhörung am 03.06.2024**

HK2 Rechtsanwälte

Umsetzungsfrist für EU-Mitgliedstaaten

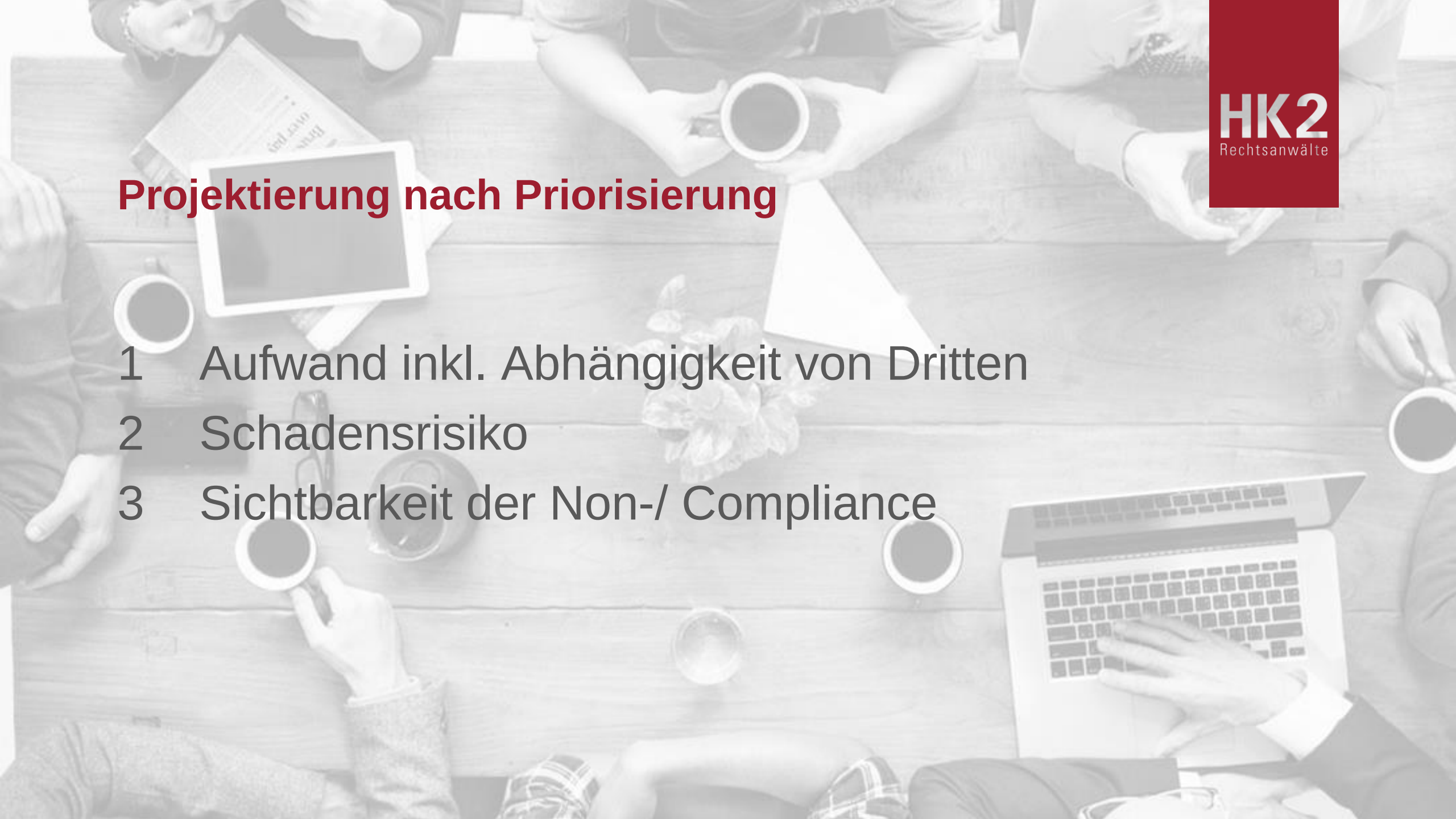
Artikel 41

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

Projektierung nach Priorisierung

1 Aufwand inkl. Abhängigkeit von Dritten

2 Schadensrisiko

3 Sichtbarkeit der Non-/ Compliance

Rechtliche Aufgaben zur NIS-2-Umsetzung

Anwendbarkeits-Prüfung: ist 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!

4 Beispiele rechtlicher Aufgaben

1. Rechtliche Aufgaben zum Risikomanagement
2. Vereinbarungen zum Stand der Technik
3. Vorbereitungen zur Rechenschaftspflicht
4. Haftung der Geschäftsleitung vermeiden

Supushpitha Atapattu /pexels.com

Technische und organisatorische Maßnahme
Mindestanforderungen, § 30 Abs. 2 BSIG-E

1. **Konzepte** in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik
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 Abs. 2 BSIG-E

6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik
7. grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich der Sicherheit in der Informationstechnik
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.

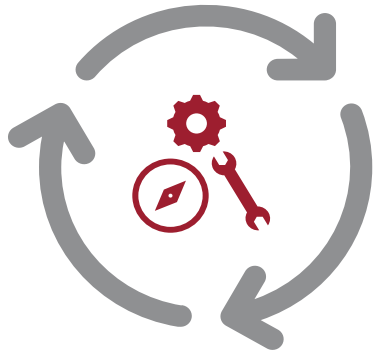
Rechtliche Prüfung, § 30 Abs. 2 BSIG-E

HK2 Rechtsanwälte

	Risikomanagementmaßnahme	Rechtliche Prüfung betrifft u. a.	Beispiele
1	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik		
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	**Prüfung der Verträge über IT-Leistungen mit Sicherheitsbezügen:** - **Beschaffung/ Einkauf von Software (SaaS/ Cloud/ On Premises, …)** - **SLA/ Wartung/ Pflege** - **Endkundenvertrag** - **Datenschutzvereinbarungen** - **…**	**Qualität und Aktualität der Vertragsmuster:** - **Umgang mit Stand der Technik** - **Leistungsbeschreibung** - **Durchsetzbarkeit der Sicherheitsleistungen** - **Anpassbarkeit** - **IT-Compliance-Klausel** - **IT-Sicherheit als Neben-/ Hauptleistung** - **Umgang mit fremden AGB, …**
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen		
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik		
7	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik		
8	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung		
9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen		
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gege-benenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung		

Technische und organisatorische Maßnahmen
§ 30 Abs. 2 BSIG-E

„(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 …“*



Stand der Technik

HK2
Rechtsanwälte

§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Dabei sind das Ausmaß der Risikoexposition die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

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 Ei
sind verpflichtet, die von diesen Einrichtungen zu
managementmaßnahmen im Bereich der Cybers
zu überwachen. Die Beauftragung eines Dritte
Satz 1 ist nicht zulässig.

(2) Geschäft
tung für den entst
ger Einrichtungen

(3) Ein Verzi
der Einrichtung üb
tige zahlungsunfä
bigern vergleicht

(4) Die Gesc
tungen müssen u
ausreichende Ker
wie Risikomanage
auf die von der Ei

**Billigungs-, Überw
besonders wi**

(1) Geschäftsleitung
Einrichtungen sind verpfl
Risikomanagementmaßn
Umsetzung zu überwache

(2) Ein Verzicht der
Pflichten nach Absatz 1
unwirksam. Dies gilt nic

Abwendung des Insolve
Ersatzpflicht in einem Ins

(3) Die Geschäftsl
Einrichtungen müssen
Kenntnisse und Fähigk
Risikomanagementpraktik
Auswirkungen von Risike
erbrachten Dienste zu erv

§ 38

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

(1) Geschäftsleitungen 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 in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis stehender 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 Geschäftsleitungen 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 Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben.

HK2 Rechtsanwälte

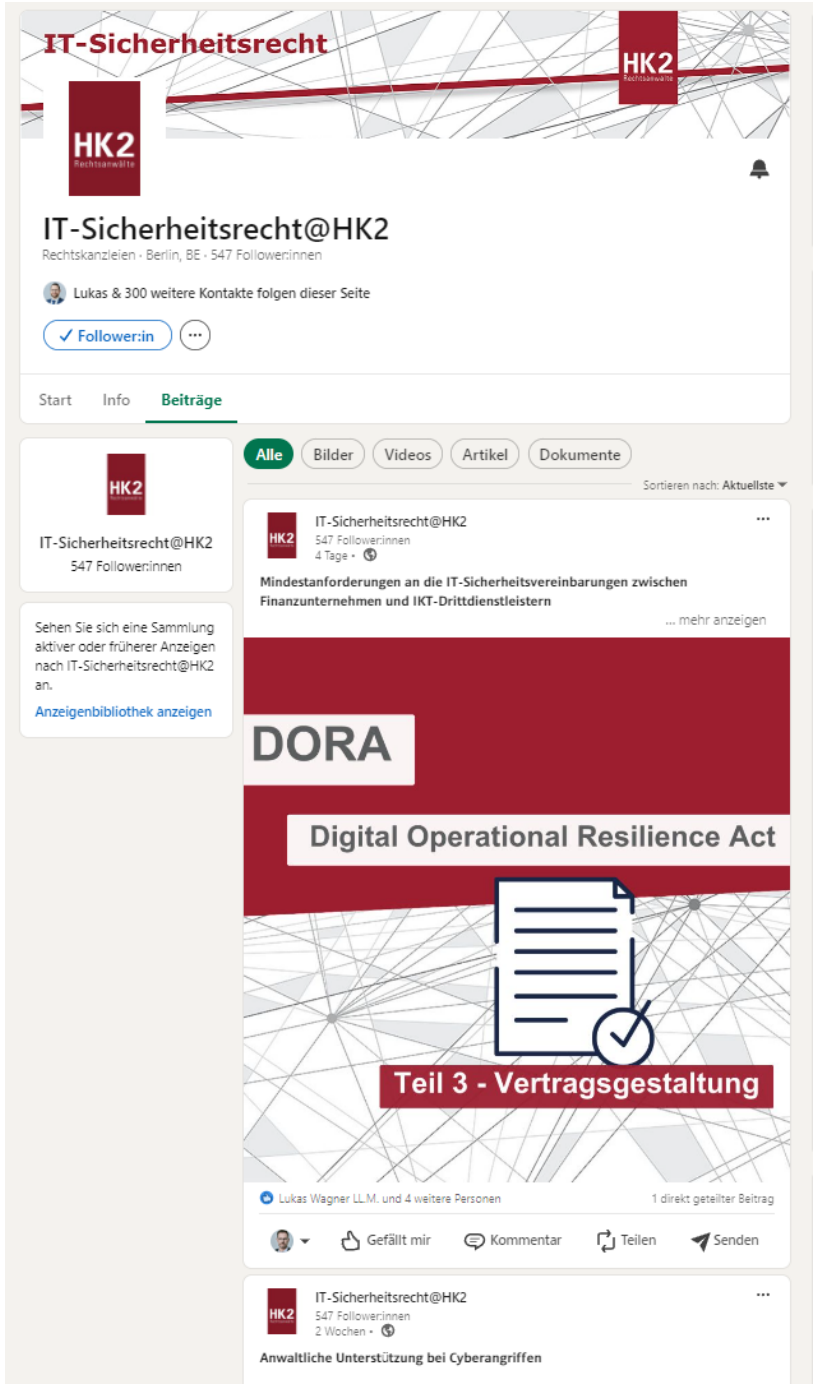
Haftung der Geschäftsleitung

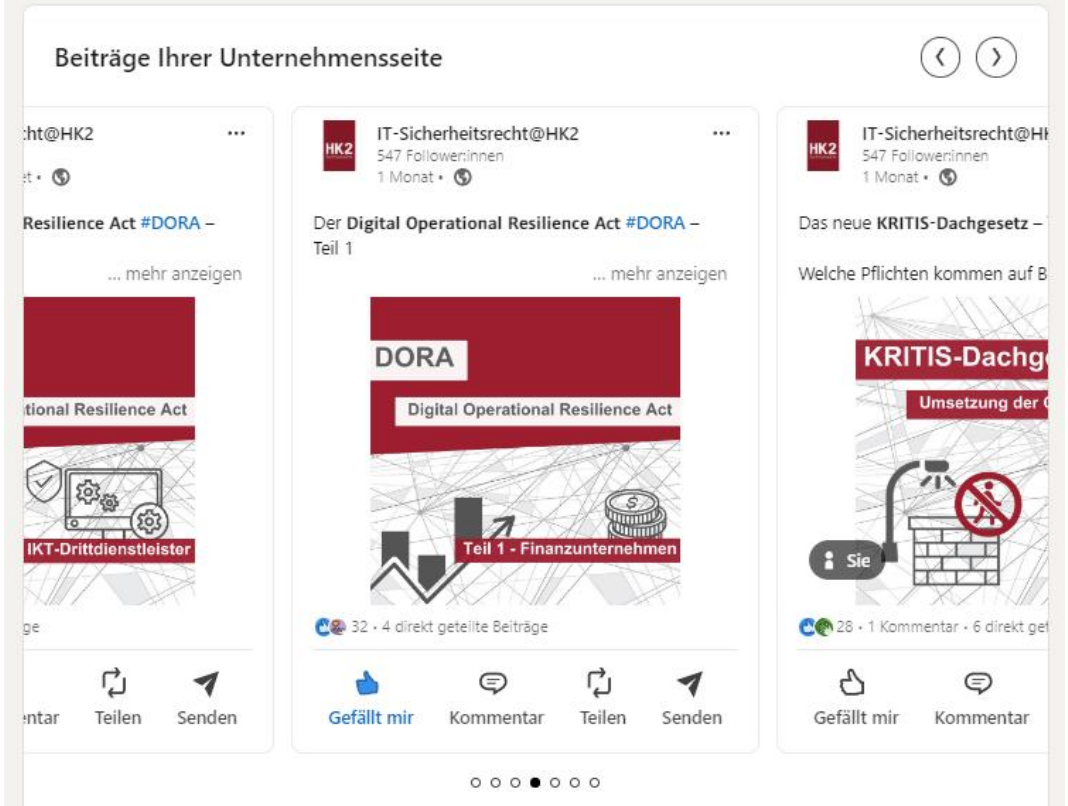
§ 65 Abs. 9 BSIG-E

Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes … trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen. In diesem Fall kann die zuständige Aufsichtsbehörde

1. die Genehmigung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung vorübergehend aussetzen und

2. natürlichen Personen die Ausübung von Leitungsaufgaben auf Geschäftsführungs- oder Vorstandsebene oder Ebene des rechtlichen Vertreters untersagen.





LinkedIn-Fokusseite

HK2
Rechtsanwälte

Kontakt

www.hk2.eu

www.comtection.de

linkedin.com/in/karstenbartels