T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Update zum IT-Sicherheitsrecht

RA Karsten U. Bartels LL.M.
HK2 Rechtsanwälte
Stellv. TeleTrusT-Vorsitzender

Karsten U. Bartels LL.M.*

- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- 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 TeleTrusT
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik


HK2
IT- und Datenrecht
Technik-Recht
IT-Sicherheitsrecht
Datenschutzrecht

IT-Sicherheitsrecht@HK2

Wir setzen IT-Sicherheit rechtlich um. Langjährige Expertise im IT-Sicherheitsrecht: gesamte Lieferkette und KRITIS.

Rechtskanzleien · Berlin, BE · 835 Follower:innen

Nachricht | ✓ Follower:in | ···

Start | Info | Beiträge

Übersicht

NIS-2-Umsetzungsberatung: Planung und rechtliche Umsetzung des NIS2UmsuCG, KRITIS-Dachgesetz und künftigem Cyber Resilience Act. Für wichtige und besonders wichtige Einrichtungen (sowie Betreiber kritischer Anlagen). IT-Sicherheitsvereinbarungen: Verträge über IT-Sicherheit als Haup ... ... mehr anzeigen

Alle Details anzeigen →

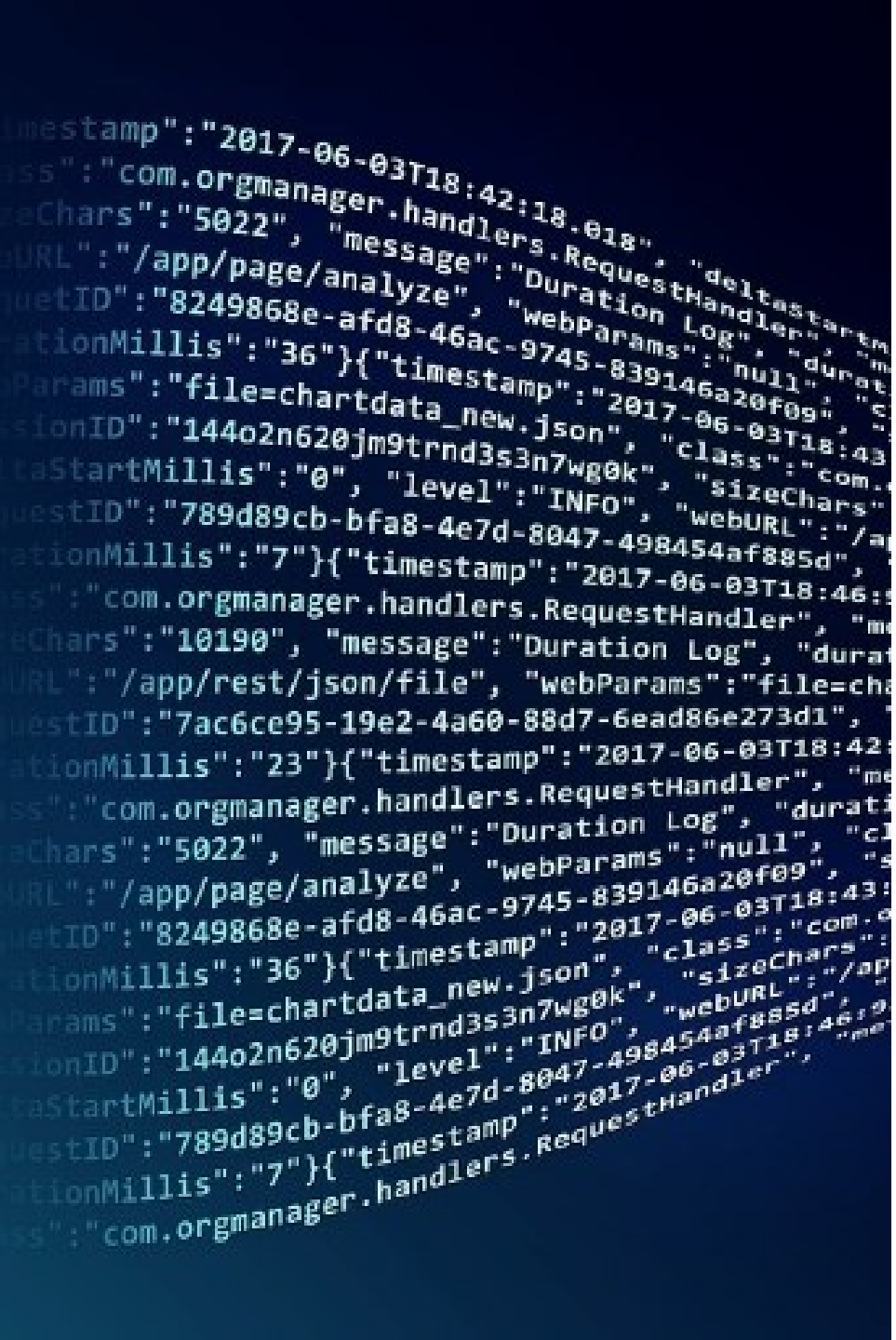
Im Fokus

1 Monat • Bearbeitet •

Für Managed Service Provider und Managed Security Service Provider gilt: NIS-2 + Sonderregeln! #MSP und #MSSP unterfallen bei entsprechender Unternehmensgröße dem kommenden ... mehr

HK2 Rechtsanwälte

LinkedIn-Fokusseite



Datenschutzbeauftragte für die IT-Branche

HK2 Comtection

- Datenschutzbeauftragte für wichtige/ besonders wichtige Einrichtungen
- Datenschutz für KRITIS-Betreiber und Zulieferer

www.comtection.de

Update IT-Sicherheitsrecht

1. Es wächst! Neue IT-Sicherheitsgesetze
2. Umgang mit Rechtslage im Unternehmen
3. NIS2UmsuCG
4. Sonderregeln
5. IT-Sicherheitsvereinbarungen
6. Falle: Nachweisfrist

HK2 Rechtsanwälte

Supushpitha Atapattu /pexels.com

Update IT-Sicherheitsrecht

1. Es wächst! Neue IT-Sicherheitsgesetze
2. Umgang mit Rechtslage im Unternehmen
3. NIS2UmsuCG
   - Stand der Gesetzgebung
   - Problem: Anwendbarkeit
   - Betroffene Vertragsverhältnisse
   - Risikomanagementmaßnahmen
4. Sonderregeln
5. IT-Sicherheitsvereinbarungen
6. Falle: Nachweisfrist

Update IT-Sicherheitsrecht

1. Es wächst! Neue IT-Sicherheitsgesetze
2. Umgang mit Rechtslage im Unternehmen
3. NIS2UmsuCG
   - Stand der Gesetzgebung
   - Problem: Anwendbarkeit
   - Betroffene Vertragsverhältnisse
   - Risikomanagementmaßnahmen
4. Sonderregeln
   - KRITIS
   - Sektoren
   - digitale Infrastruktur
5. IT-Sicherheitsvereinbarungen
6. Falle: Nachweisfrist

IT-Sicherheitsgesetze

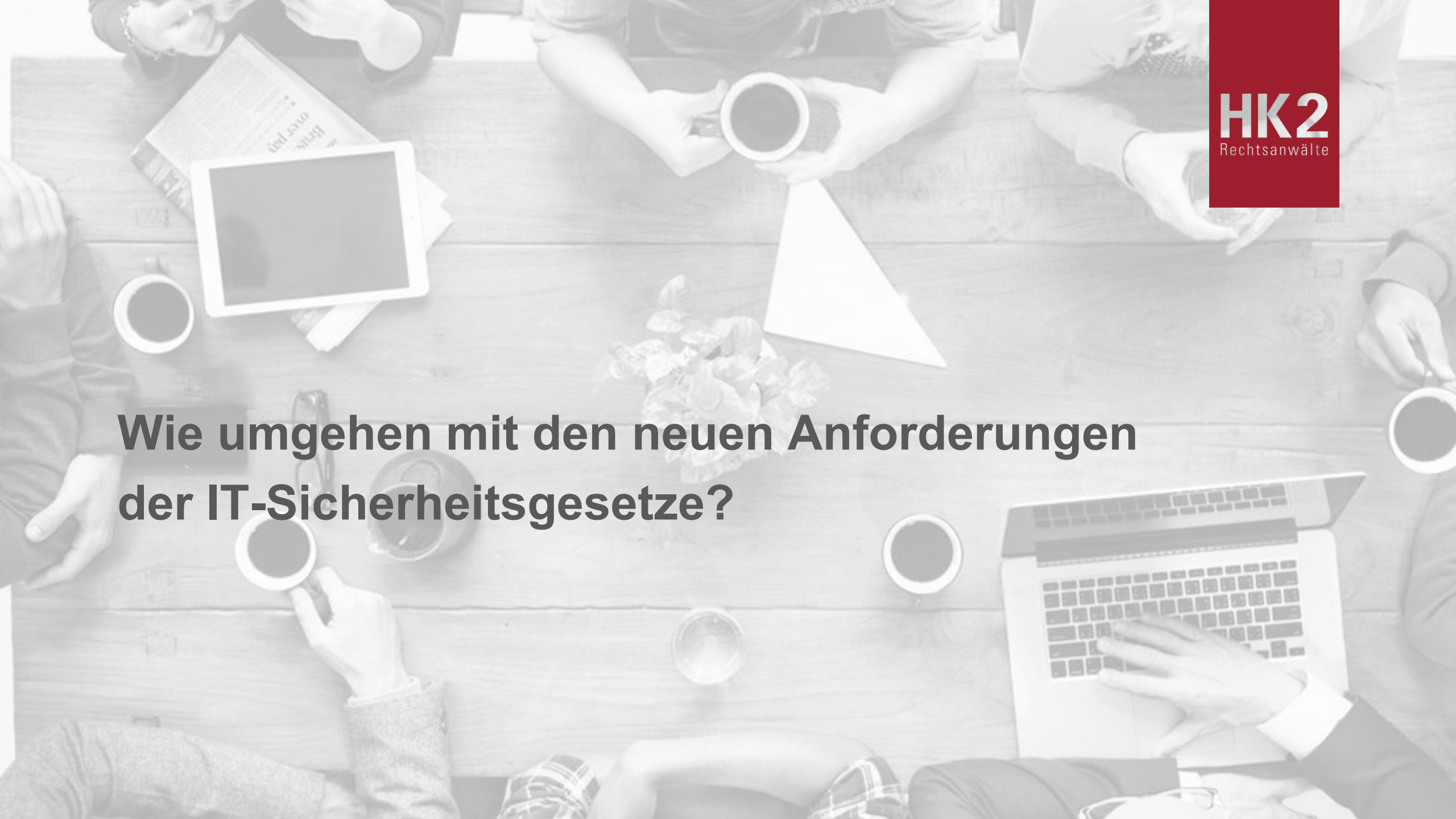
NIS-2

NIS2UmsuCG

HK2
Rechtsanwälte

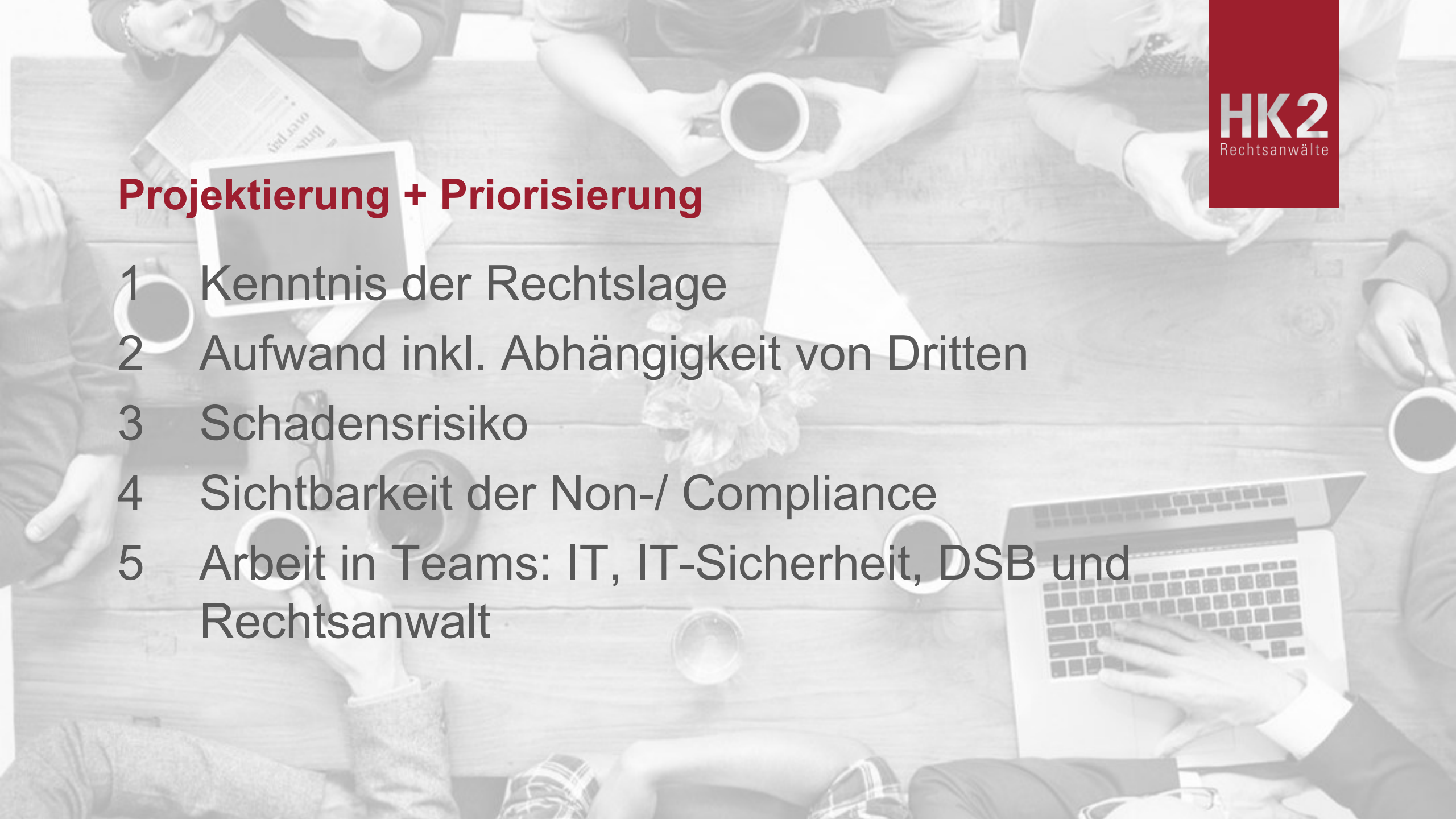

HK2
Rechtsanwälte
NIS2UmsuCG
OZG
KRITIS-DachG
DSGVO
EnWG
TDDDG
BSIG
CRA
Data Act
DORA
BSI-KRITIS-VO
BGB
GeschGehG
RED
DSA
TKG
eIDAS 2.0
KI-Verordnung
CSA
SGB
AtomG


HK2
Rechtsanwälte
NIS2UmsuCG
OZG
KRITIS-DachG
DSGVO
EnWG
TDDDG
BSIG
CRA
Data Act
DORA
BSI-KRITIS-VO
BGB
GeschGehG
RED
DSA
TKG
eIDAS 2.0
KI-Verordnung
CSA
SGB
AtomG



HK2
Rechtsanwälte

Wie umgehen mit den neuen Anforderungen der IT-Sicherheitsgesetze?

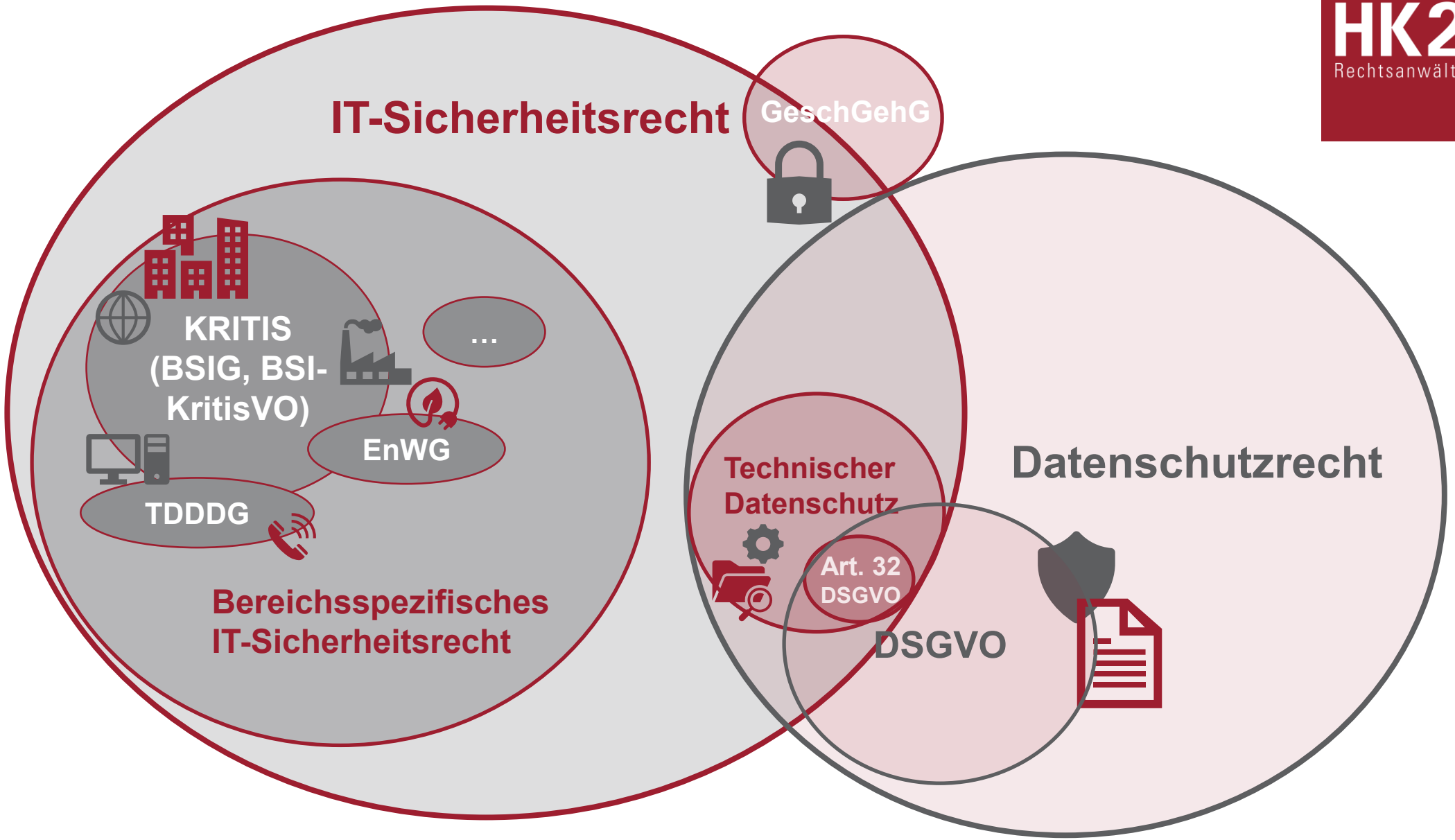


HK2 Rechtsanwälte

Projektierung + Priorisierung

1. Kenntnis der Rechtslage
2. Aufwand inkl. Abhängigkeit von Dritten
3. Schadensrisiko
4. Sichtbarkeit der Non-/ Compliance
5. Arbeit in Teams: IT, IT-Sicherheit, DSB und Rechtsanwalt

HK2
Rechtsanwälte



Stand des Gesetzgebungsverfahrens zum NIS2UmsuCG

HK2 Rechtsanwälte

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

BMI und Regierungsentwurf

- Referentenentwurf vom 07.05.2024
- Stellungnahmen bis zum 28.05.2024
- Anhörung der Länder am 31.05.2024
- Anhörung der Verbände am 03.06.2024
- 4. Ref-Entwurf (erster offizieller) vom 07.05.2024
- 5. Ref-Entwurf vom 24.06.2024
- Gesetzesentwurf der Bundesregierung vom 19.07.2024
- Kabinettbeschluss am 24.07.2024, Entwurf vom 22.07.2024

Parlamentsverfahren

- Gesetzesentwurf der Bundesregierung vom 16.08.2024
- Stellungnahme des Bunderats v. 27.09.2024, Gegenäußerung der Bundesregierung v. 02.10.2024
- 1. Lesung im BT am 11.10.2024
- Ausschuss für Inneres und Heimat am 04.11.2024

Wer ist betroffen?

HK2
Rechtsanwälte

HK2
Rechtsanwälte

Besonders wichtige Einrichtungen

- Betreiber kritischer Anlagen

Wichtige Einrichtungen

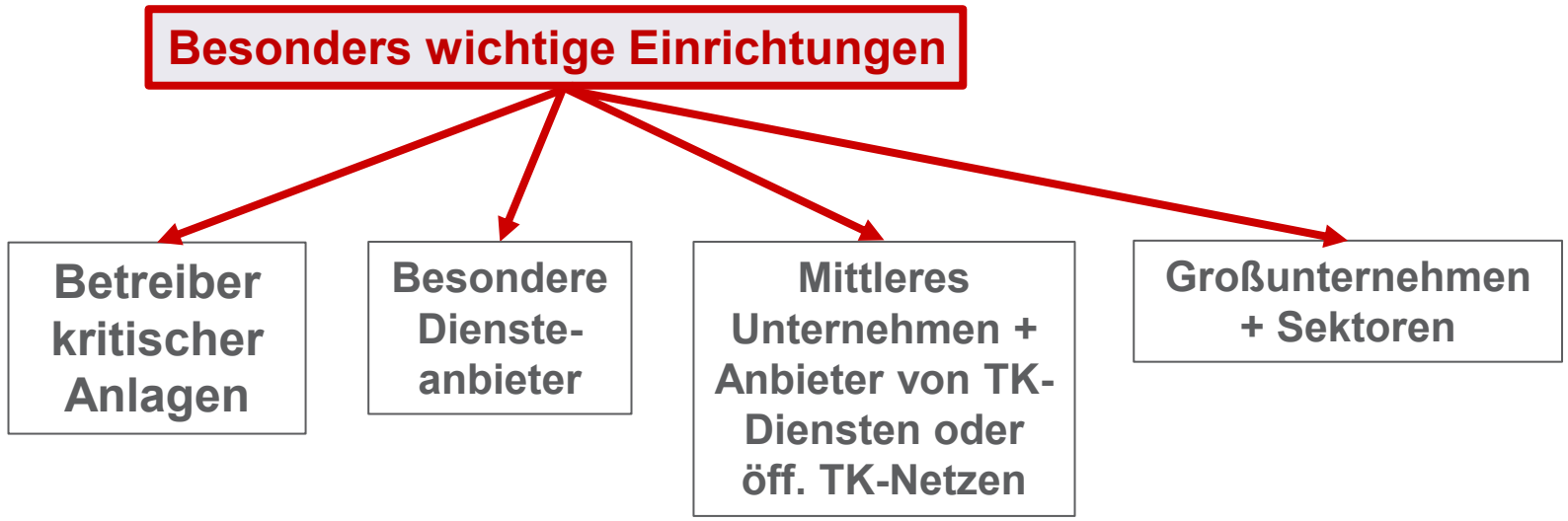
HK2 Rechtsanwälte

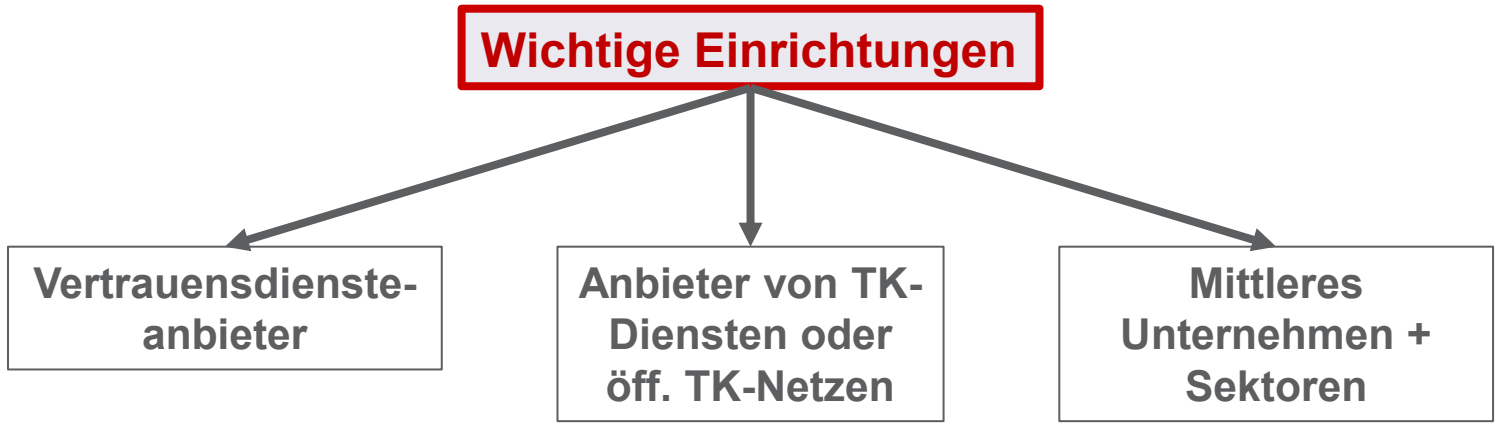
Besonders wichtige Einrichtungen

Betreiber kritischer Anlagen

Wie zuvor: Nähere Bestimmung der kritischen Anlagen durch **Rechtsverordnung** gem. **§ 56 Abs. 4 BSIG-E**

HK2 Rechtsanwälte





→ Einrichtungsarten der verschiedenen Sektoren jetzt in **Anlagen 1 und 2.** Zudem **Rechtsverordnung** gem. **§ 56 Abs. 4** BSIG-E

HK2 Rechtsanwälte

Das NIS2UmsuCG – Unternehmen im BSIG-E

Großunternehmen
§ 28 Abs. 1 Nr. 4 BSIG-E

250+ oder

und

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

Mittlere Unternehmen
§ 28 Abs. 1 Nr. 3 und
Abs. 2 Nr. 3 BSIG-E

50+ oder

und

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

Kleine Unternehmen (TK)
§ 28 Abs. 2 Nr. 2 BSIG-E

<50 und

und

<10 Mio. **<10 Mio.**

Besonders wichtige Einrichtungen

Grahame Jenkins/Unsplash.com

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen, § 28 Abs. 1 BSIG-E

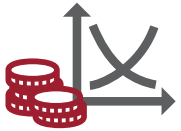
- **Betreiber kritischer Anlagen** (i. V. m. § 28 Abs. 7)
- **Qualifizierter Vertrauensdiensteanbieter**, **TLD Name Registries** oder **DNS-Diensteanbieter** (unabhängig von Unternehmensgröße)
- **Mittleres Unternehmen,** das Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder Betreiber öffentlicher Telekommunikationsnetzen ist
- **Großunternehmen**, das einer Einrichtungsart eines relevanten Sektors zuzuordnen ist (i. V. m. Anlage 1)

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Betreiber kritischer Anlagen


Energie


Ernährung


Finanzwesen


Sozialvers.tr./ Grundsich. f. Arbeitssuchend.


Vertr.diensteanb (qual./normal)

Abfallbewirtschaftung


Forschung


Wasser


IT und TK


Transport und Verkehr


TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Weltraum


Gesundheit


Siedlungsabfall-entsorgung


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

DNS-Diensteanb.

Lebensmittel

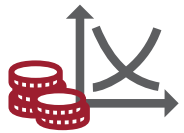

Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Großunternehmen


Energie


Ernährung


Finanzwesen

Sozialvers.tr./ Grundsich. f. Arbeitssuchend.


Vertr.diensteanb (qual./normal)

Abfallbewirtschaftung


Forschung


Wasser


IT und TK


Transport und Verkehr

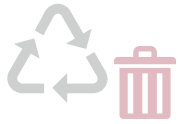

TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Weltraum


Gesundheit


Siedlungsabfallentsorgung


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

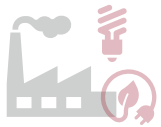
DNS-Diensteanb.

Lebensmittel

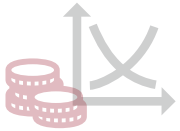

Anb. digitaler Dienste

HK2 Rechtsanwälte

Besonders wichtige Einrichtungen – Mittlere Unternehmen


Energie


Ernährung


Finanzwesen

Sozialvers.tr./ Grundsich. f. Arbeitssuchend.

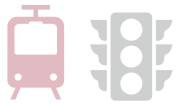

Vertr.diensteanb (qual./normal)

Abfallbewirtschaftung


Forschung

Wasser

IT und TK


Transport und Verkehr

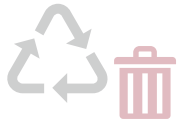

TLD Name Registries


Chemie

Verarbeitendes Gewerbe


Weltraum


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 Abs. 2 BSIG-E

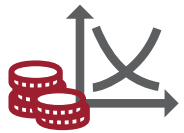
- **Mittleres Unternehmen,** das einer Einrichtungsart eines relevanten Sektors zuzuordnen ist (i. V. m. Anlagen 1 und 2)
- **Kleinunternehmen,** das Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder Betreiber öffentlicher Telekommunikationsnetzen ist
- **Vertrauensdiensteanbieter**

HK2 Rechtsanwälte

Wichtige Einrichtungen – Mittlere Unternehmen


Energie


Ernährung


Finanzwesen

Sozialvers.tr./ Grundsich. f. Arbeitssuchend.


Vertr.diensteanb (qual./normal)


Abfallbewirtschaftung


Forschung


Wasser


IT und TK


Transport und Verkehr

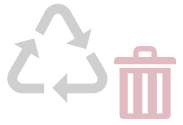

TLD Name Registries


Chemie


Verarbeitendes Gewerbe


Weltraum


Gesundheit


Siedlungsabfall-entsorgung


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

DNS-Diensteanb.


Lebensmittel


Anb. digitaler Dienste

HK2 Rechtsanwälte

Anwendbarkeit des NIS2UmsuCG ist:

1. von **Unternehmen** zu prüfen
2. stark **einzelfallabhängig**
3. **komplex**, z. B. konzerninternen Leistungen, Auslandsbezug oder Mehrfachregulierung
4. **eine Rechtsfrage**
   - ✓ **Gutachten**
   - ✓ **Einzelaspekte**
   - ✓ **Second Opinion**

HK2
Rechtsanwälte

§ 28 BSIG-Entwurf

(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf

1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und
2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20. Mai 2003, S. 36) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.

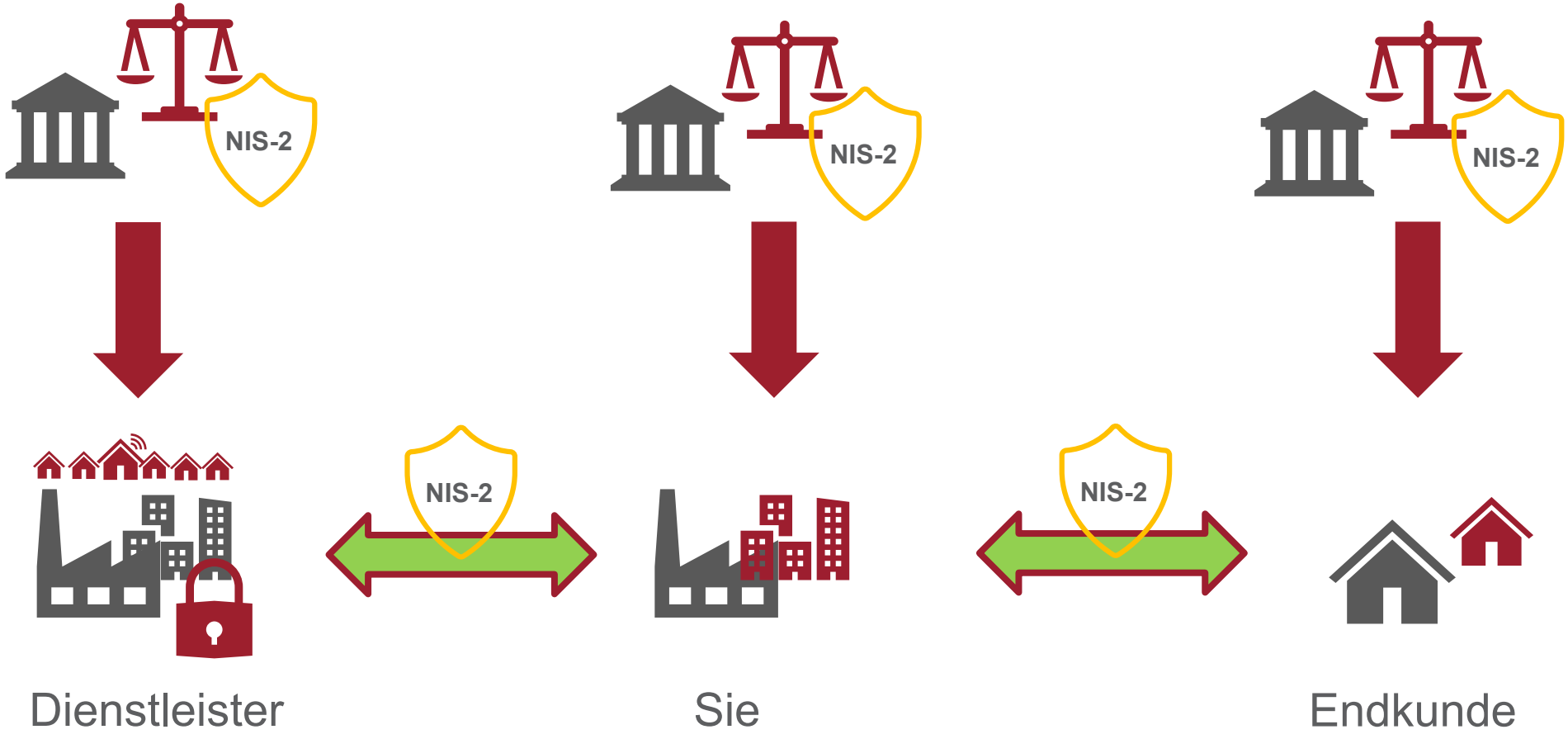
Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.

Betroffene Vertragsverhältnisse

HK2
Rechtsanwälte

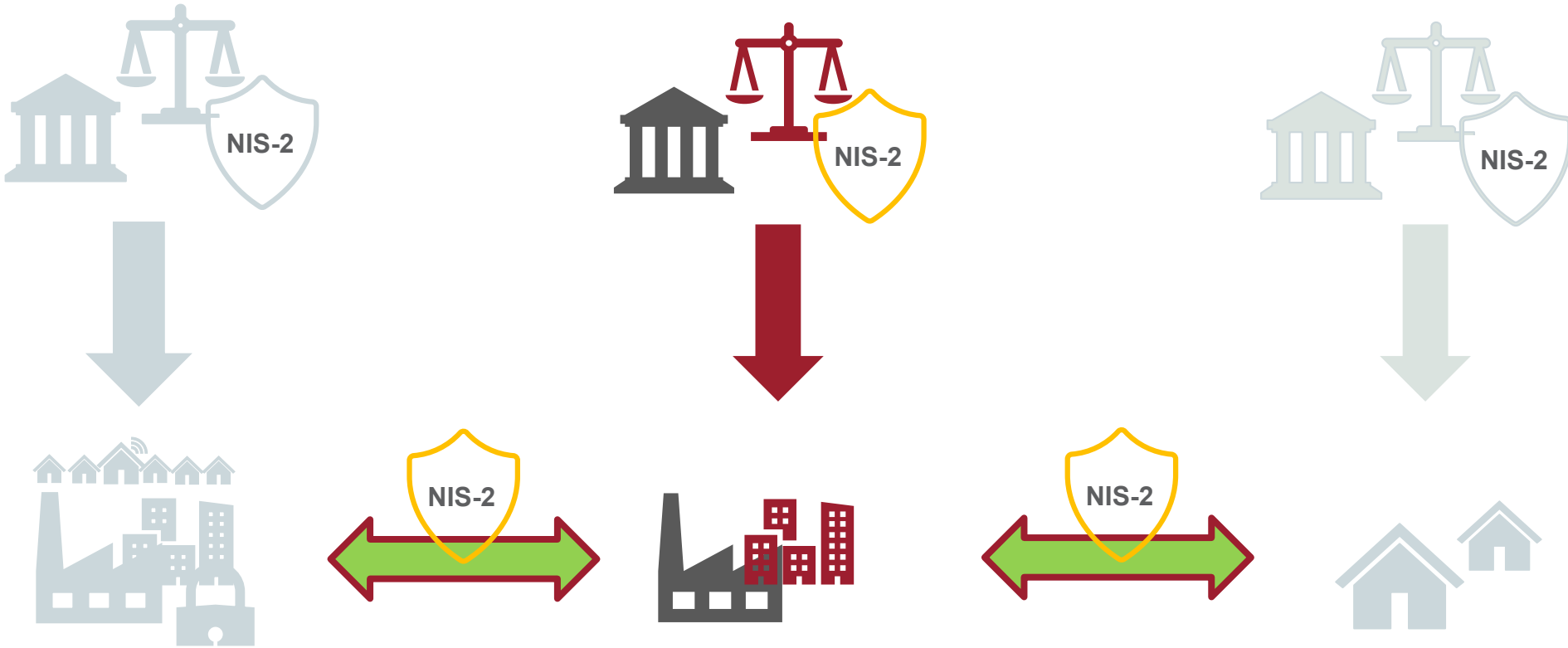
HK2
Rechtsanwälte

Vertikale Pflichten. Horizontale Pflichten.



HK2
Rechtsanwälte

Vertikale Pflichten. Horizontale Pflichten.



HK2
Rechtsanwälte

IT-Compliance durch Technik, Organisation + Recht

Verträge zur IT-Sicherheit

Verträge zur IT-Sicherheit

Dienstleister

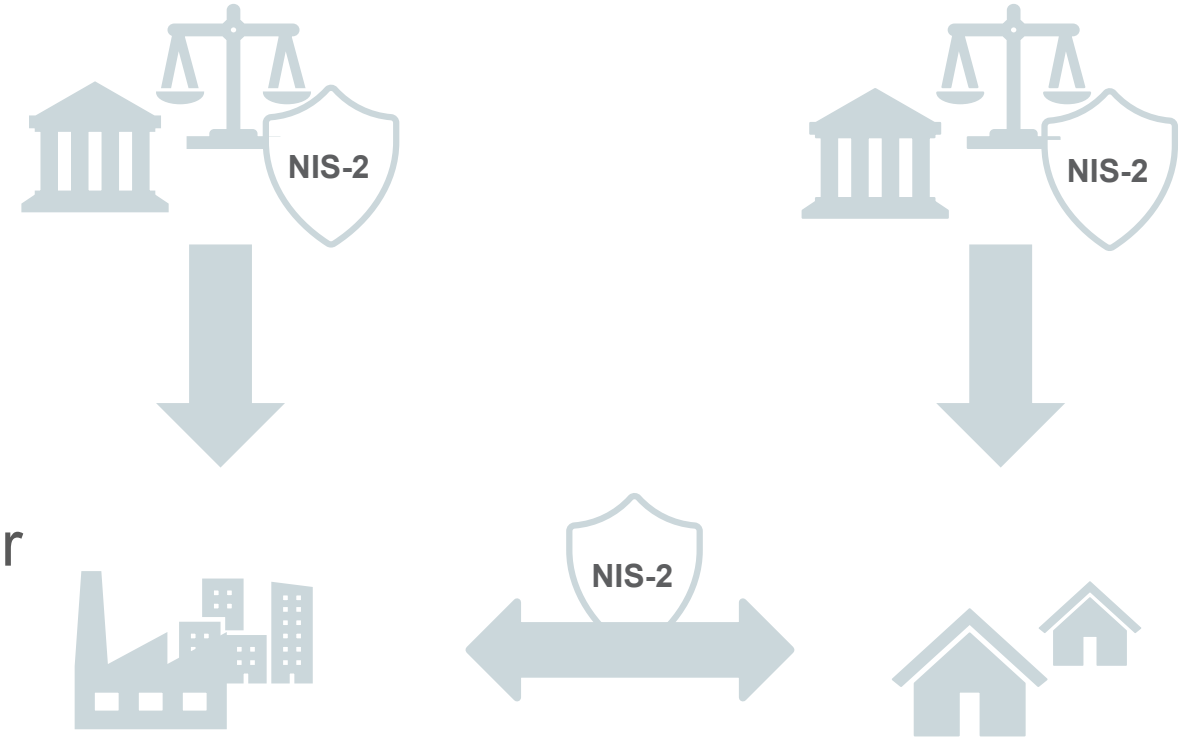
Sie

Endkunde

HK2 Rechtsanwälte

Was ist zu tun? Verträge zur IT-Sicherheit anpassen!

- Einkaufs-/ Verkaufsbedingungen
- Andere Leistungsverträge
- Konzerninterne Verträge
- Service Level Agreements
- Datenschutzvereinbarungen
- weitere Vereinbarungen über IT-Sicherheitsleistungen
- Ausschreibungsunterlagen



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

- Risikomanagementmaßnahmen
- Meldepflichten
- Registrierungspflicht
- Unterrichtungspflicht
- Umsetzungs-, Überwachungs- und Schulungspflicht
- Nachweispflichten für KRITIS-Betreiber
- und mehr…

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

- 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**
- bleibt möglich: Branchenspezifische Sicherheitsstandards (B3S), Abs. 9

Technische und organisatorische Maßnahme Mindestanforderungen, § 30 Abs. 2 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**

HK2 Rechtsanwälte

Technische und organisatorische Maßnahme Mindestanforderungen, § 30 Abs. 2 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.

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 gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung		

HK2 Rechtsanwälte

Weitere besondere Pflichten für Betreiber kritischer Anlagen §§ 31, 41 BSIG-E

- Aufwändigere Maßnahmen grds. verhältnismäßig, § 31 Abs. 1 BSIG-E

- Systeme zur Angriffserkennung, § 31 Abs. 2 BSIG-E
  - definiert in § 2 Nr. 41 BSIG-E
  - Identifizierung von Bedrohungen
  - Stand der Technik, aber verhältnismäßiger Aufwand

- Einsatz kritischer Komponenten, § 41 BSIG-E
  - definiert in § 2 Nr. 23 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)

Weitergehende Risikomanagementmaßnahmen für Betreiber kritischer Anlagen, § 31 BSIG-E

HK2 Rechtsanwälte

(1) Für Betreiber kritischer Anlagen **gelten** für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch über das Schutzniveau dieser Einrichtungen hinausgehende **Maßnahmen** nach § 30 Absatz 1 Satz 1 **als verhältnismäßig**, **wenn** der dafür erforderliche Aufwand **nicht außer Verhältnis** zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

(2) …

BSIG-E vs. EnWG

HK2 Rechtsanwälte

	Risikomanagementmaßnahme § 30 Abs. 2 BSIG-E	**IT-Sicherheitskataloge gem. § 5c EnWG-E**
1	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	*wie links*
- 10	…	
11		Einsatz von **Systemen zur Angriffserkennung** nach § 2 Nr. 41 BSIG-E
12		**Einsatz** eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (**IKT-Produkt**), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (**IKT-Dienst**) und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (**IKT-Prozess**) **mit Cybersicherheitszertifizierung** gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (ABl. 151 vom 7.6.2019, S. 15).

Weitere durch das NIS2UmsuCG geänderte Gesetze *(Auswahl)*

- **Energiewirtschaftsgesetz** (Art. 17 NIS2UmsuCG)
  - Insb. Neueinführung des § 5c EnWG-E
- **Messstellenbetriebsgesetz** (Art. 18 NIS2UmsuCG)
  - In § 24 II MsbG „Zertifizierung des Smart-Meter-Gateway“ wird § 9 des BSIG durch § 52 des BSIG-E ersetzt
- **Energiesicherungsgesetz** (Art. 19 NIS2UmsuCG)
  - Ergänzung des § 10 Abs. 1 EnSiG „Auskünfte, Datenerhebung und -übermittlung“
  - Begriffsanpassungen (z. B. „kritische Infrastruktur“ in „kritische Anlagen“)
- **Wärmeplanungsgesetz** (Art. 20 NIS2UmsuCG)
  - In § 11 IV WPG gleiche begriffliche Anpassungen wie bei EnSiG

Anforderungen an digitale Infrastruktur, § 30 BSIG-E

(3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, 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 und Vertrauensdiensteanbieter hat für die vorgenannten Einrichtungsarten Vorrang.

(4) Sofern 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 Anforderungen den in Absatz 2 genannten Maßnahmen vor, soweit sie diesen entgegenstehen.

(5) Sofern 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 über die sektoralen Anforderungen an die 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.

Durchführungsrechtsakte für Anbieter digitaler Infrastruktur

HK2 Rechtsanwälte

EUROPEAN COMMISSION

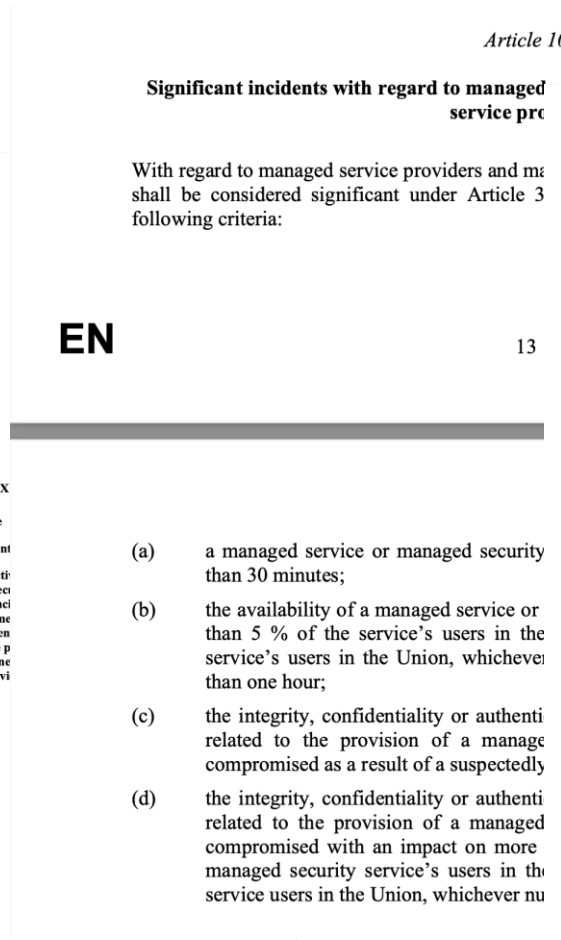
Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)



Article 10

Significant incidents with regard to managed service pro

With regard to managed service providers and ma shall be considered significant under Article 3 following criteria:

EN

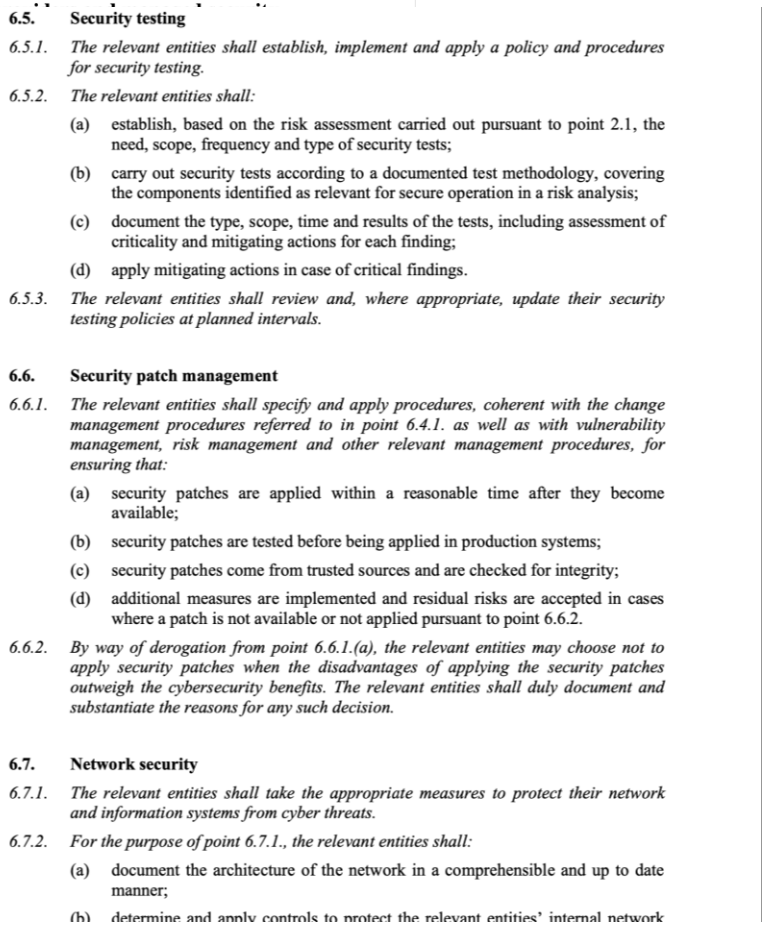
13

(a) a managed service or managed security than 30 minutes;

(b) the availability of a managed service or than 5 % of the service's users in the service's users in the Union, whichever than one hour;

(c) the integrity, confidentiality or authenti related to the provision of a manage compromised as a result of a suspectedly

(d) the integrity, confidentiality or authenti related to the provision of a managed compromised with an impact on more managed security service's users in th service users in the Union, whichever nu



6.5. Security testing

6.5.1. The relevant entities shall establish, implement and apply a policy and procedures for security testing.

6.5.2. The relevant entities shall:

(a) establish, based on the risk assessment carried out pursuant to point 2.1, the need, scope, frequency and type of security tests;

(b) carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;

(c) document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;

(d) apply mitigating actions in case of critical findings.

6.5.3. The relevant entities shall review and, where appropriate, update their security testing policies at planned intervals.

6.6. Security patch management

6.6.1. The relevant entities shall specify and apply procedures, coherent with the change management procedures referred to in point 6.4.1. as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:

(a) security patches are applied within a reasonable time after they become available;

(b) security patches are tested before being applied in production systems;

(c) security patches come from trusted sources and are checked for integrity;

(d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.

6.6.2. By way of derogation from point 6.6.1.(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision.

6.7. Network security

6.7.1. The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.

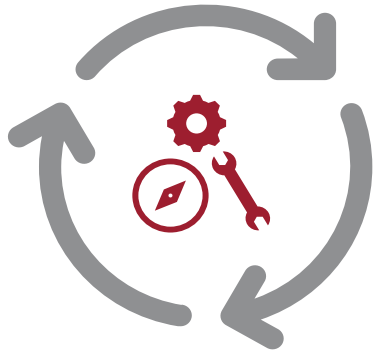
6.7.2. For the purpose of point 6.7.1., the relevant entities shall:

(a) document the architecture of the network in a comprehensible and up to date manner;

(b) determine and apply controls to protect the relevant entities' internal network

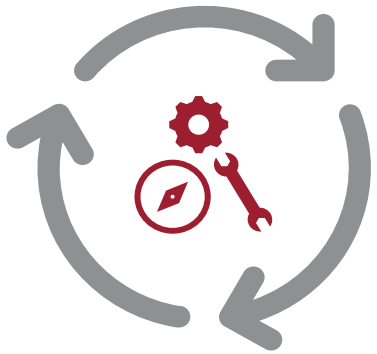
Technische und organisatorische Maßnahmen
§ 30 Abs. 2 BSIG-E

„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



Stand von Wissenschaft und Forschung

↑

Stand der Technik

↓

Allgemein anerkannte Regeln der Technik

HK2
Rechtsanwälte

Verträge zur IT-Sicherheit

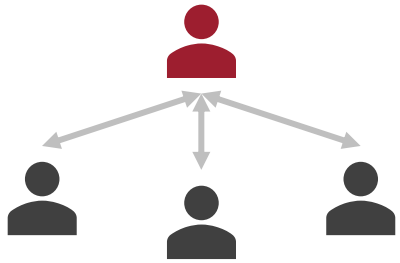
HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(unvollständig)*

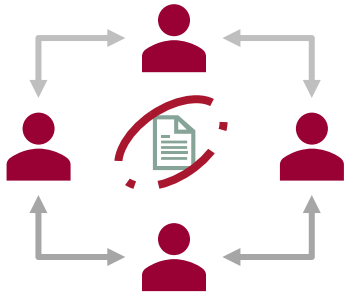
Präambel
1. Begriffsbestimmungen
2. Geltungs- und Anwendungsbereich
3. Leistungen
4. Leistungserbringung nach dem Stand der Technik
5. Weitere Anforderungen an Leistungserbringung
6. Compliance- und KRITIS-Zulieferer-Verpflichtungen
7. Dokumentationen
8. Zertifikate, Testate und Audits
9. Unterbeauftragungen
10. Geheimhaltung
11. Vertragsstrafen
12. Change Request
13. Überleitungskooperation
14. Change of control
15. Auslegung

HK2 Rechtsanwälte

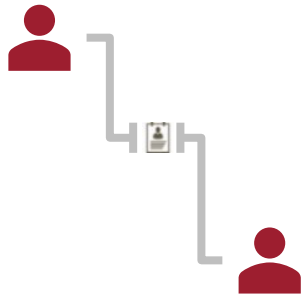
Vereinbarungen zu Datenschutz/ IT-Sicherheit



Auftragsverarbeitung



Joint controllers



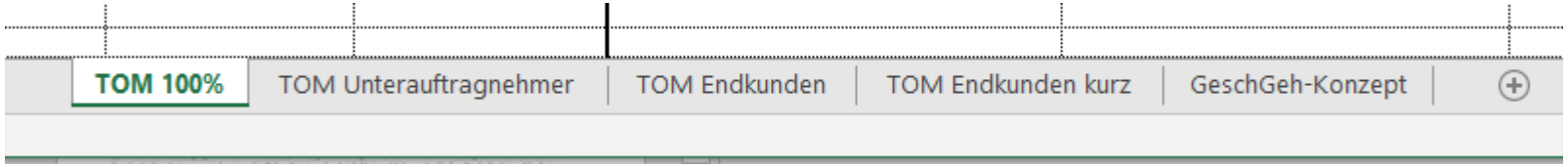
getrennt Verantwortliche

Daten ohne Personenbezug

NIS-2/ DORA/ …

HK2
Rechtsanwälte

Dokumentation



HK2 Rechtsanwälte

Nachweispflichten für Betreiber kritischer Anlagen, § 39 BSIG-E

- Nachweis der Erfüllung der Anforderungen nach §§ 30 Abs. 1 S. 1 , 31 Abs. 1, Abs. 2 S. 1 BSIG-E für KRITIS-Betreiber
- Frühestens **drei Jahre** nach erstmaliger/ erneuter Geltung als KRITIS, anschließend alle drei Jahre
- Kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen
- Übermittlung an BSI, ggf. Nachweis auch über die Beseitigung aufgetretener Mängel

Achtung: Nachweispflichten (on demand) auch für wichtige und besonders wichtige Einrichtungen

- § 61 Abs. 3, Aufsichts- und Durchsetzungsmaßnahmen für **besonders wichtige Einrichtungen**:
  - BSI kann gegenüber besonders wichtigen Einrichtungen frühestens **drei Jahre** nach Inkrafttreten des Gesetzes die Vorlage von Nachweisen über die Erfüllung bestimmter Pflichten anordnen

- Nach § 62 BSIG-E hat BSI gegenüber **wichtigen Einrichtungen** die Rechte gemäß § 61
  - Voraussetzung: Tatsachen rechtfertigen die Annahme, dass Pflichten aus § 61 nicht oder nicht richtig umgesetzt werden

HK2 Rechtsanwälte

Meldepflichten, § 32 BSIG-E

- Betrifft **besonders wichtige und wichtige Einrichtungen**
- Meldepflicht an Meldestelle bei **erheblichen Sicherheitsvorfällen**
  - Sicherheitsvorfall, § 2 Nr. 40 BSIG-E
  - Erheblicher Sicherheitsvorfall, § 2 Nr. 11 BSIG-E
- Mehrstufiges Meldeverfahren in Abs. 1
- Zusätzliche Meldepflicht für KRITIS-Betreiber in Abs. 3

HK2 Rechtsanwälte

Meldepflichten, § 32 Abs. 1 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

Umsetzungs-, Überwachungs- und Schulungspflicht für Leitungsorgane, § 38 BSIG-E

- Pflicht der Geschäftsleiter hinsichtlich Umsetzung TOM. Zudem Umsetzung zu überwachen.
- Bei Verletzung der Umsetzungspflichten nach gesellschaftsrechtlichen Vorschriften; Haftung nach dem BSIG-E, wenn gesellschaftsrechtliche Vorschriften keine Haftungsregelungen enthalten
- Geschäftsleiter haben regelmäßig an Schulungen teilzunehmen

§ 38

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

(1)
sind verp
manager
zu überv
Satz 1 is

(2)
tung für
ger Einri

(3)
der Einri
tige zahl
bigern ve

(4)
tungen r
ausreich
wie Risik
auf die v

§ 38

Umsetzungs-, 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 umzusetzen und ihre Umsetzung zu überwachen.

(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(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 und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

erbrachten Dienste zu erwerbe

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

HK2 Rechtsanwälte

Haftung der Geschäftsleitung

§ 61 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. Die zuständige Aufsichtsbehörde kann, …, als letztes Mittel

1. die dieser Einrichtung erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen und

2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Absatz 1 Nummer 13), vorübergehend untersagen

HK2 Rechtsanwälte

Rechtliche Aufgaben zum NIS2UmsuCG

Anwendbarkeits-Prüfung. Auch für konzernverbundene Unternehmen.

Geschäftsleitung einbeziehen + schulen!

„Risikomanagementmaßnahmen“ gem. § 30 BSIG-E prüfen/ umsetzen/ anpassen.

Ist Kunde betroffen? IT-Sicherheitsvereinbarungen mit Kunden + Kommunikation anpassen.

IT-Sicherheit mit Zulieferern/ Dienstleistern verhandeln!

Datenschutz anpassen.

HK2
Rechtsanwälte

Wer verhandelt gerade IT-Sicherheit?

HK2
Rechtsanwälte

Melden Sie sich gern

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