HK2 Rechtsanwälte

IT-Sicherheitsvereinbarungen –

wie man IT-Sicherheit technisch und rechtlich richtig verhandelt und vereinbart

RA Karsten U. Bartels LL.M.

Omnisecure Tutorial, 21.01.2025

HK2
Rechtsanwälte

Karsten U. Bartels LL.M.*

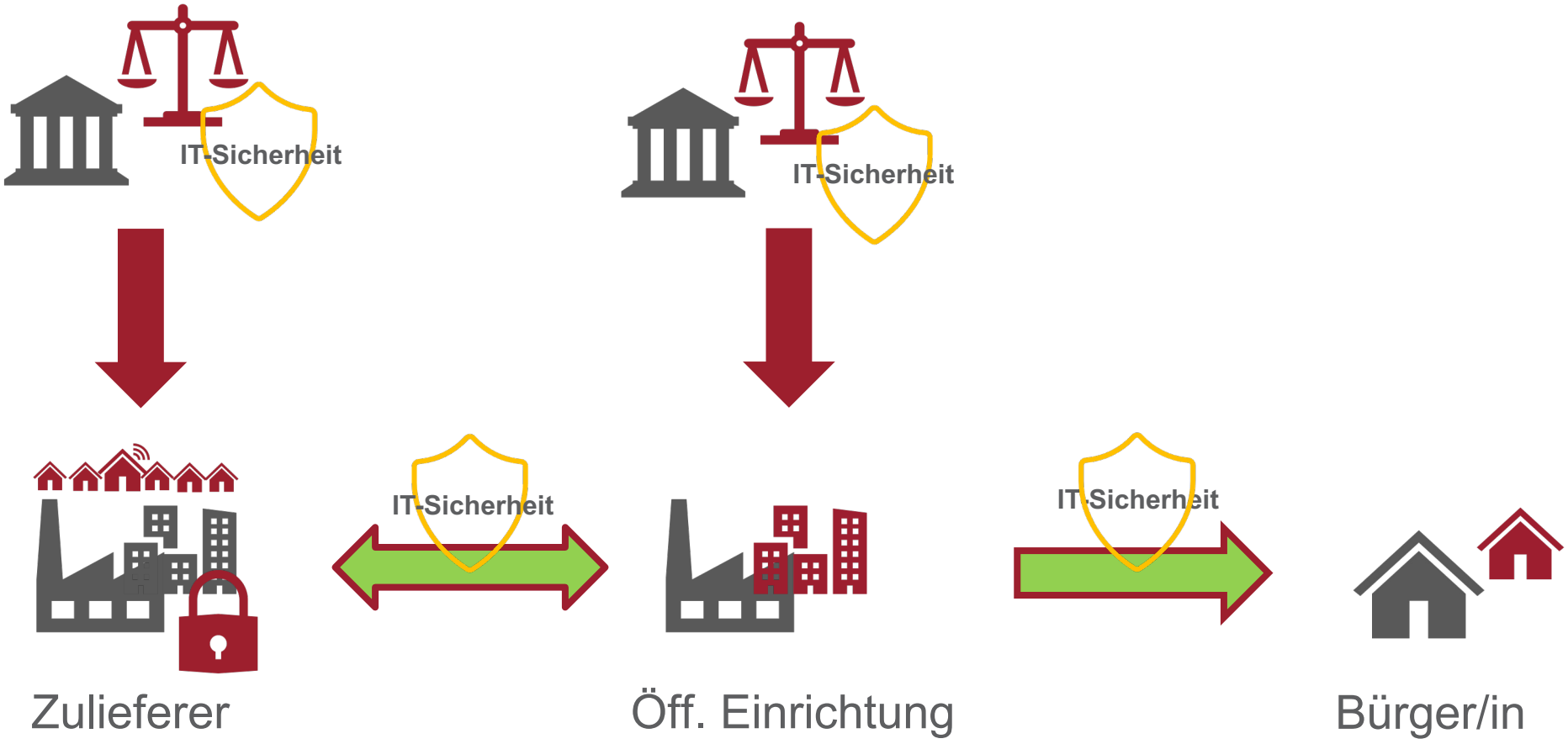
- Rechtsanwalt/ Partner bei HK2
- Geschäftsführer HK2 Comtection GmbH
- Lehrbeauftragter für IT-Sicherheitsrecht, Ludwig-Maximilians-Universität München
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit (TeleTrusT)
- Leiter AG IT-Sicherheitsrecht TeleTrusT
- Vorsitzender Arbeitsgemeinschaft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

*Rechtsinformatik


HK2
Rechtsanwälte
DORA
NIS-2-DurchfRA
NIS2UmsuCG
BDSG
OZG
KRITIS-DachG
DSGVO
TDDDG
BSIG
CRA
EnWG
Data Act
CSA
BSI-KRITIS-VO
BGB
GeschGehG
DSA
RED
TKG
eIDAS 2.0
KI-Verordnung
DDG
SGB V
AtomG

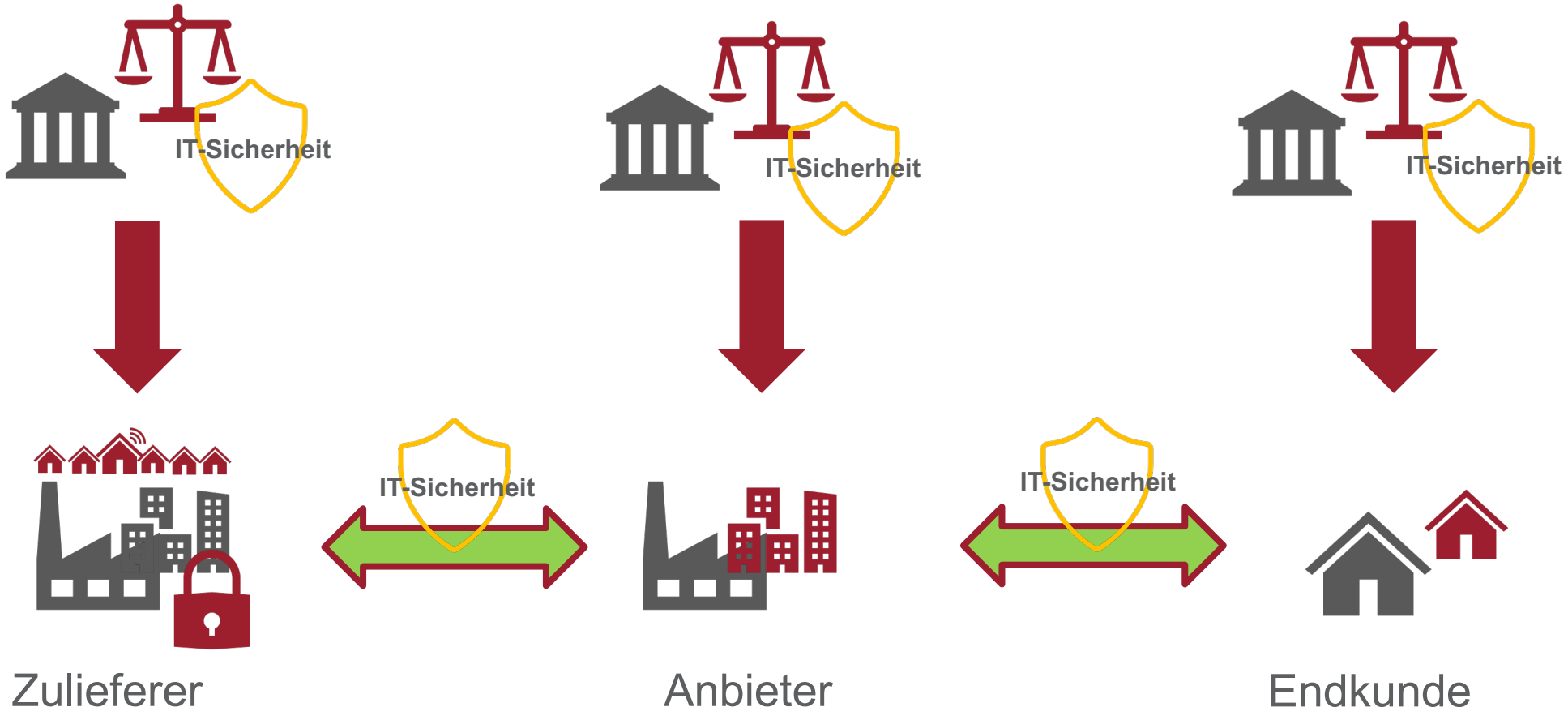
HK2
Rechtsanwälte

IT-Sicherheitsvereinbarungen: wer?



HK2
Rechtsanwälte

IT-Sicherheitsvereinbarungen: wer?



HK2
Rechtsanwälte

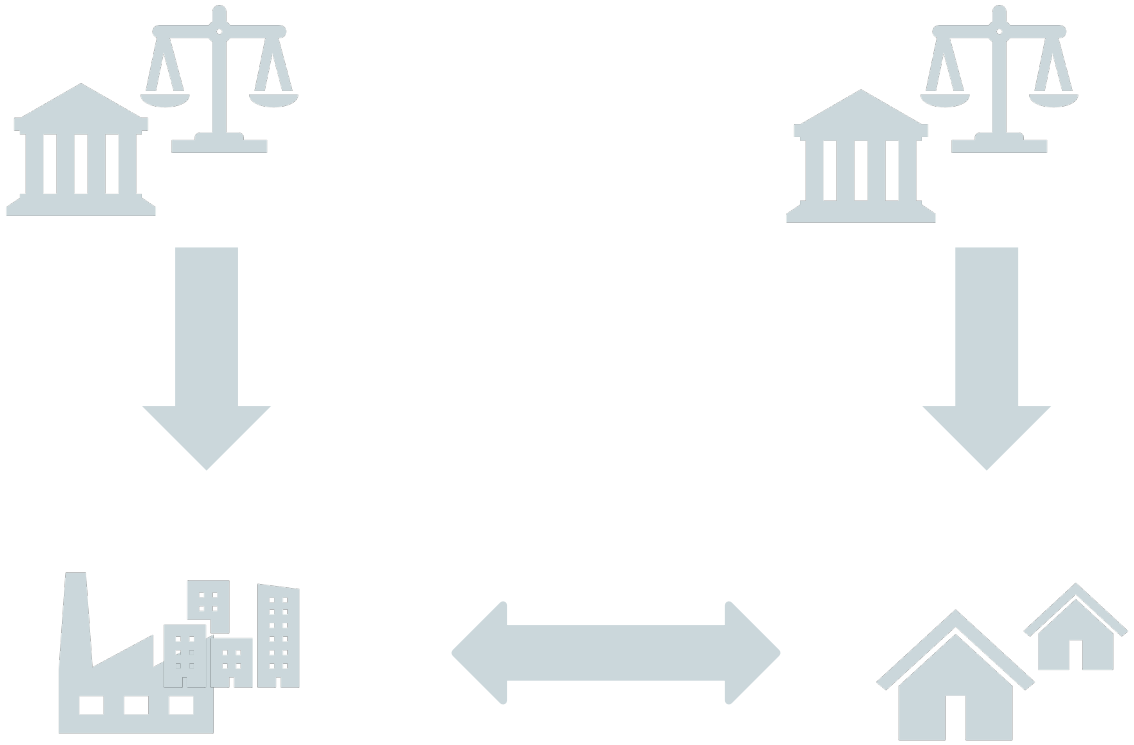
Agenda

HK2
Rechtsanwälte

Verträge zur IT-Sicherheit

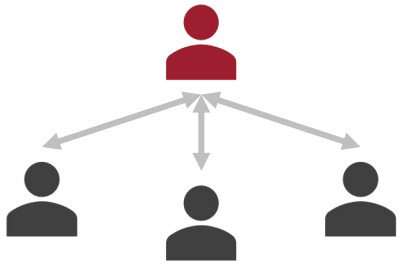
- Leistungsverträge
- Individuelle Verträge/ AGB
- Ausschreibungsunterlagen
- Service Level Agreements
- Vereinbarungen nach DSGVO
- Weitere Vereinbarungen über IT-Sicherheitsleistungen
- Geheimhaltungsvereinbarungen

- *betrifft ggf. auch Geschäftsmodell*

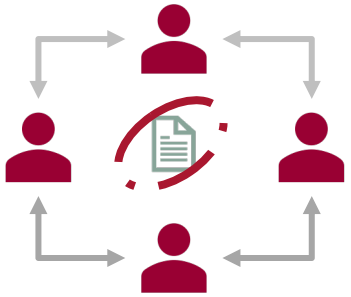


HK2
Rechtsanwälte

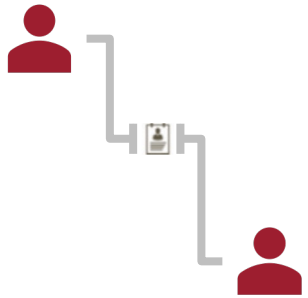
Vereinbarungen sind aufeinander abzustimmen



Auftragsverarbeitung



Joint controllers



getrennt Verantwortliche

Daten ohne Personenbezug

NIS-2/ DORA/ KI-VO/ CRA/ …

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2 Rechtsanwälte

Schwachstelle

Art. 6 Ziff. 15 NIS-2-Richtlinie (RL 2022/2555/EU)

„Schwachstelle“ ist eine **Schwäche**, **Anfälligkeit** oder **Fehlfunktion** von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann.

§ 2 Nr. 38 NIS2UmsuCG-E

„Schwachstelle“ [ist] eine **Eigenschaft** von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich **gegen den Willen des Berechtigten Zugang** zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die **Funktion** der IKT-Produkte oder IKT-Dienste zu beeinflussen.

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2 Rechtsanwälte

Schwachstellen-Management

Schwachstellen

- erkennen
- bewerten + priorisieren
- beheben/ zeitweise abmildern
- reporten

Auch: Umgang mit Cyberbedrohungen

Schwachstellenmanagement gemäß Art. 13 Abs. 3 i. V. m. Anhang I Teil II Cyber Resilience Act

HK2 Rechtsanwälte

Teil II Anforderungen an die Behandlung von Schwachstellen

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten der Produkte mit digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen;

(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen teilen und veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie eindeutige und verständliche Informationen, die den Nutzern helfen, die Schwachstellen zu beheben; in hinreichend begründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden;

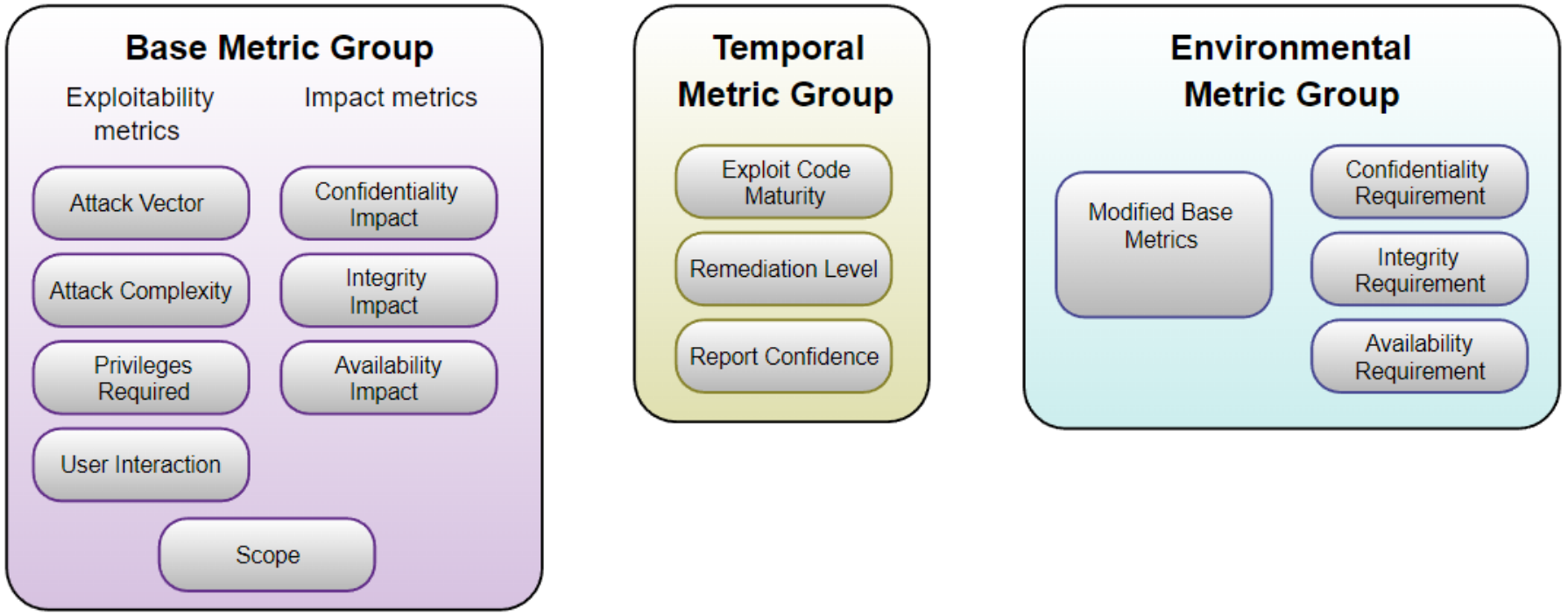
(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;

(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;

(7) Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitstellen, damit Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen gegebenenfalls automatisch behoben oder eingedämmt werden;

(8) dafür sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und — sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde — kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

Bsp. Methode zur Schwachstellenbewertung
Common Vulnerability Scoring System (CVSS)



https://www.first.org/cvss/v3.1/specification-document

Incident Management

- Routine-Untersuchung
- forensische Maßnahmen
- Beschreibung nach vereinbartem Schema
- Verfügbarkeit/ Unterstützung für/ bei Abhilfe

Durchführungsrechtsakt der EU Kommission vom 17.10.2024

Artikel 7

Erhebliche Sicherheitsvorfälle in Bezug auf Anbieter von Cloud-Computing-Diensten

In Bezug auf Anbieter von Cloud-Computing-Diensten gilt ein Sicherheitsvorfall als erheblich im Sinne von Artikel 3 Absatz 1 Buchstabe g, wenn er eines oder mehrere der folgenden Kriterien erfüllt:

a) ein erbrachter Cloud-Computing-Dienst ist mehr als 30 Minuten lang vollständig nicht verfügbar;

b) die Verfügbarkeit eines Cloud-Computing-Dienstes eines Anbieters ist für mehr als 5 % der Nutzer des Cloud-Computing-Dienstes in der Union oder für mehr als 1 Mio. Nutzer des Cloud-Computing-Dienstes in der Union — je nachdem, welche Zahl niedriger ist — für eine Dauer von mehr als einer Stunde eingeschränkt;

c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Cloud-Computing-Dienstes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;

d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Cloud-Computing-Dienstes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer des Cloud-Computing-Dienstes in der Union oder auf mehr als 1 Mio. Nutzer des Cloud-Computing-Dienstes in der Union — je nachdem, welche Zahl niedriger ist — aus.

g) der Vorfall erfüllt eines oder mehrere der in den Artikeln 5 bis 14 aufgeführten Kriterien.

Beispiele wichtiger TOM

- SBOM (Software Bill of Materials) v. a. gegen die aktuellen Supply-Chain-Attacken
- SIEM (Security Information and Event Management)/ Log Management
- Geo-Redundanzen gem. Standort-Kriterien für RZ nach BSI
- Zero-Trust-Maßnahmen
- Kryptoagilität sicherstellen
- …

ESB Professional/Shutterstock.com

Rechtliche Prüfung, § 30 Abs. 2 BSIG-E

HK2 Rechtsanwälte

	Risikomanagementmaßnahme	**Rechtliche Prüfung betrifft u. a.**
1	Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	Bewertung der Konzepte anhand der IT-sicherheitsgesetzlichen Vorgaben
2	Bewältigung von Sicherheitsvorfällen	Bewertung des Vorgehensmodells bei Sicherheitsvorfällen
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	Bewertung der beschriebenen Maßnahmen/ Konzepte
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** - **…**
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	Bewertung: 1. der Konzepte/ Verfahren IT-sicherheitsrechtlich bestehen und 2., ob Vorgehen mit Vertragspartnern vereinbart wird.
7	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik	Bewertung der Schulungslage: wie wird wer mittels welcher Inhalte zur IT-Compliance geschult?
8	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung	Prüfung zu vertraglichen Regelungen zur Verschlüsselung
9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen	Prüfung der Maßnahmen zur Auswahl des Personals
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gege- benenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	Bewertung der Verpflichtung und Schulung der Mitarbeiter

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

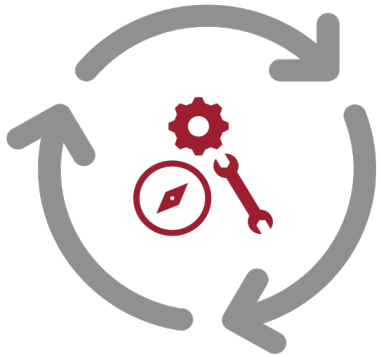
HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

Beim Stand der Technik handelt es sich um die im Waren- und Dienstleistungsverkehr **verfügbaren** Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen **gesetzlichen Schutzziele** am **wirkungsvollsten gewährleisten** kann.



[Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht - Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress, S. 503]

HK2
Rechtsanwälte

www.stand-der-technik-security.de/

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2 Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. Vertragsstrafen
13. Änderungen der Leistungspflichten während der Laufzeit (Change Request)
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

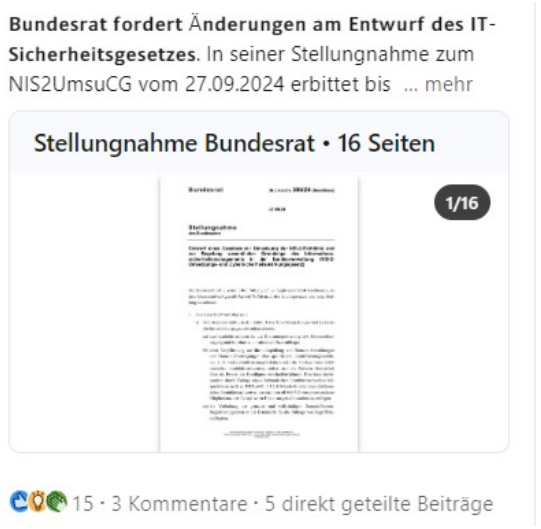
IT-Sicherheitsvereinbarung
Gliederung *(Auszug)*

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. Ansprechpartner, Weisungen, Mitarbeiter
11. Geheimhaltung, Datenschutz
12. **Vertragsstrafen**
13. **Änderungen der Leistungspflichten während der Laufzeit (Change Request)**
14. Überleitungskooperation
15. Change of control
16. Auslegung
17. Anlagen

HK2
Rechtsanwälte

Wer verhandelt gerade IT-Sicherheit?

HK2
Rechtsanwälte



LinkedIn-Fokusseite

HK2
Rechtsanwälte

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