T.I.S.P. Community Meeting 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 05. - 06.11.2019

Stand der Technik nach IT-Sicherheitsgesetz 2.0 und DSGVO

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte, Vorstand TeleTrusT

Karsten U. Bartels LL.M.*

- Rechtsanwalt und Partner bei HK2 Rechtsanwälte
- Geschäftsführer HK2 Comtection GmbH
- Vorsitzender AG IT-Recht (davit) im Deutschen Anwaltverein e. V.
- Stellv. Vorstandsvorsitzender Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Zert. Datenschutzbeauftragter (TÜV)

*Rechtsinformatik

HK2
Rechtsanwälte

Zum Einstieg …

eine Bestandsaufnahme.

HK2
Rechtsanwälte

Wie gehen derzeit Unternehmen und Behörden in der EU mit dem *Stand der Technik* um?

HK2
Rechtsanwälte

Unvertretbar schlecht.

sdecoret/Shutterstock.com

Gründe

1. unklare Gesetze
2. keine relavante aufsichtsbehördliche Unterstützung
3. historische begründete Scheinsicherheit
4. unklare Zuständigkeiten (IT, Recht, DSB, CISO)
5. Fehleinschätzung der gesetzlichen Pflichten
6. Außerachtlassung vorhandener Methoden
7. Verträge nicht *state of the art*

Agenda

- Stand der Technik
  - DSGVO
  - IT-Sicherheitsgesetz
  - Telemediengesetz
  - Geschäftsgeheimnisschutzgesetz?
- Umsetzung
  - Definition
  - Feststellung
  - Angemessenheit
  - Dokumentation
- Haftung
- Vertragliches

Sicherheit der Verarbeitung
Art. 32 DSGVO

HK2 Rechtsanwälte

Gewährleistung eines dem Risiko angemessenen Schutzniveaus

Geeignete technische und organisatorische Maßnahmen (TOM)

berücksichtigen

- Eintrittswahrscheinlichkeit und Schwere des Risikos einer Rechtsverletzung des Betroffenen (*Schutzbedarfsanalyse*)
- Art, Umfang, Umstände, Zweck der Verarbeitung
- Stand der Technik 

Panumas nikhomkhai/Pexel

HK2 Rechtsanwälte

Stand von Wissenschaft und Forschung

Stand der Technik

Allgemein anerkannte Regeln der Technik

HK2 Rechtsanwälte

Stand der Technik ist ...

… der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.

[Gesetzesbegründung zu § 8a BSIG, BT-Drucks. 18/4096, S. 26]

HK2 Rechtsanwälte

Stand der Technik ist ...

… der Entwicklungsstand **fortschrittlicher** Verfahren, Einrichtungen oder Betriebsweisen, der die **praktische Eignung** einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der **Verfügbarkeit, Integrität, Authentizität** und **Vertraulichkeit gesichert erscheinen lässt**.

[Gesetzesbegründung zu § 8a BSIG, BT-Drucks. 18/4096, S. 26]

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

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

Kurz:

Stand der Technik = die am Markt verfügbare Bestleistung zur Erreichung eines gesetzlichen IT-Sicherheitszieles.

Fragenkatalog zur Ermittlung des Stands der Technik

HK2 Rechtsanwälte

1. Maßnahmenbeschreibung und IT-Sicherheitsziele
2. verfügbare Dokumentationen
3. Bezug auf Standards/ Normungen
4. Empfehlungen von Fachverbänden/ Experten
5. Regelmäßige Überprüfung der Maßnahme
6. Grad der Fortschrittlichkeit
7. Praxiserprobung
8. Vergleichbare Maßnahmen

HK2
Rechtsanwälte

TeleTrusT
Pioneers in IT security.
1989 30 Jahre 2019
Bundesverband IT-Sicherheit e.V.

TeleTrusT auf Twitter | TeleTrusT auf LinkedIn | Impressum | Datenschutzerklärung |

TeleTrusT

Sie sind hier: Arbeitsgremien » Recht / Technik / Design / Platform » Stand der Technik

- Startseite
- TeleTrusT-Positionen
- IT-Sicherheitsstrategie
- IT-Sicherheitsgesetz
- **Arbeitsgremien**
  - Biometrie
  - Blockchain
  - Cloud Security
  - EBCA-Technik
  - ECSO
  - Forum elektronische Vertrauensdienste AK A
  - Gesundheitstelematik
  - IT Security made in Germany
  - ISM
  - Marktforschung

Arbeitskreis "Stand der Technik"

Tomasz Lawicki, Schwerhoff Consultants
RA Karsten U. Bartels, LL.M., HK2 Rechtsanwälte

Der TeleTrusT-Arbeitskreis "Stand der Technik" wurde 2015 als Untergremium der TeleTrusT-AG "Recht" initiiert. Die Gründung folgte der Forderung des IT-Sicherheitsgesetzes, den "Stand der Technik" bei technischen und organisatorischen Vorkehrungen in Unternehmen zu berücksichtigen bzw. einzuhalten. Inzwischen fordert auch die EU-Datenschutz-Grundverordnung die Orientierung am Stand der Technik (Art. 32). Seitens des Gesetzgebers wurde jedoch bislang keine Konkretisierung des Technologieniveaus geliefert. Dies gilt nicht nur für Unternehmen, sondern auch für Behörden bzw. öffentliche Stellen.

Seit seiner Etablierung ist der TeleTrusT-AK "Stand der Technik" bestrebt, betroffenen Unternehmen, Anbietern und Diensteistern Hilfestellung bei der Bestimmung des "Standes der Technik" zu geben. Daraus resultierend wurde 2016 die 1. Version der TeleTrusT-Handreichung "Stand der Technik" veröffentlicht, in der die technischen und organisatorischen Maßnahmen spezifiziert beschrieben sind.

Um die Aktualität des Dokumentes sicherzustellen, sieht sich der Arbeitskreis der Fortschreibung verpflichtet.

HK2
Rechtsanwälte

teletrust.de/stand-der-technik/

HK2
Rechtsanwälte

Inhalt der Handreichung: Regulatorisches, Methoden, Maßnahmen

HK2 Rechtsanwälte

Technische Maßnahmen

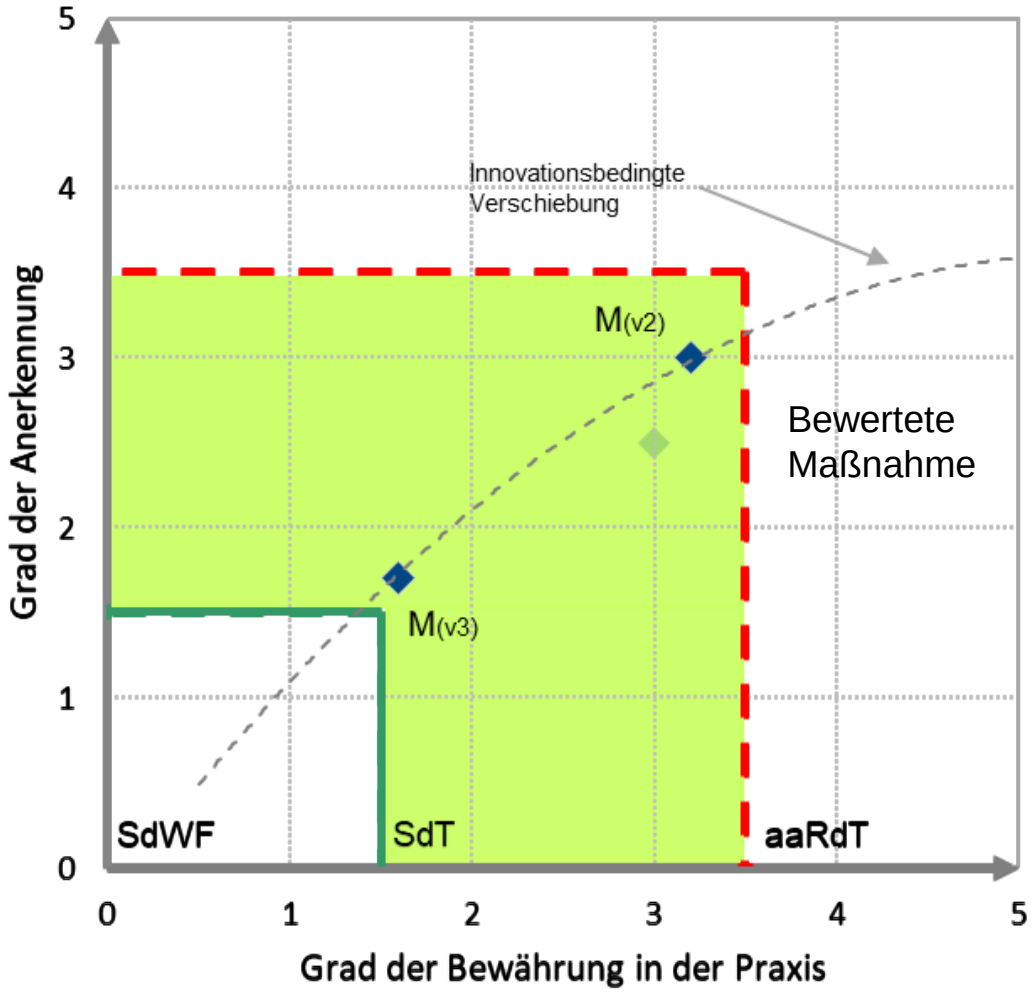
- Bewertung der Passwortstärke, Multi-Faktor-Authentifizierung
- Serverhärtung
- Verschlüsselung von Festplatten, Dateien, E-Mails
- Cloudbasierter Datenaustausch
- Datenablage in der Cloud
- Nutzung von mobilen Sprach- und Datendiensten
- Kommunikation mittels Instant-Messenger
- Management mobile Geräte
- Routersicherheit
- Verschlüsselung auf Layer 2 / Layer 3
- Netzwerküberwachung mittels Intrusion Detection System (IDS)
- Fernzugriff auf Netzwerke/ Fernwartung
- Endpoint Detection & Response Platform (EDR)
- etc.

Organisatorische Maßnahmen

- Standards and Normen
- Prozesse
  - Sicherheitsorganisation
  - Anforderungsmanagement
  - Risikomanagement
  - Ressourcenmanagement
  - IT-Servicemanagement
  - etc.
- Sichere Softwareentwicklung
- Audits and Zertifizierung
- Schwachstellen- und Patchmanagement

HK2 Rechtsanwälte

Kategorie	Leitfrage	Bewertung
Dokumentations-Stand	Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung?	1 Wiss. Publikation 3 Fachmedien 5 Massenmedien
Normenbezug	Nimmt die Maßnahme Bezug auf internationale oder nationale Normen?	1 Nein, noch nicht normiert 3 Ja, eine 5 Ja, mehr als eine
Einsatz-Empfehlung	Wurde die Maßnahme von anerkannten Gremien / Verbänden empfohlen?	1 Nein, noch nicht 3 Ja, führenden 5 Ja, vielen
Überprüfung	Wird die Eignung der Maßnahme regelmäßig überprüft?	1 Nein, noch nicht 3 Ja, herstellerseitig 5 Ja, unabhängige Instanz



M (v3) = TLS 1.3

M (v2) = TLS 1.2

M (v1) = TLS 1.0 (nicht mehr sichtbar)

Verhältnis zu untergesetzlichen Normen, Zertifikaten

HK2 Rechtsanwälte

- technische Normen und Richtlinien
  - BSI IT-Grundschutz
  - ISO 27001 u. a.
- Zertifizierungen gem. Art. 42 ff. DSGVO

Sicherheit der Verarbeitung
Art. 32 DSGVO

HK2 Rechtsanwälte

Gewährleistung eines dem Risiko angemessenen Schutzniveaus

Geeignete technische und organisatorische Maßnahmen (TOM)

berücksichtigen

- Eintrittswahrscheinlichkeit und Schwere des Risikos einer Rechtsverletzung des Betroffenen (*Schutzbedarfsanalyse*)
- Art, Umfang, Umstände, Zweck der Verarbeitung
- Stand der Technik  Wirksamkeitsprüfung, …

HK2 Rechtsanwälte

Art. 32 Abs. 1 DSGVO

… diese Maßnahmen schließen unter anderem Folgendes ein:

…

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Sicherheit der Verarbeitung
Art. 32 DSGVO

Berücksichtigen des Stands der Technik Art. 32 Abs. 1 DSGVO

1. Wissen
2. Fachliche Bewertung
3. Schlussfolgerung

Angemessenheits-kriterien: technisch


Herstaub/Shutterstock.com

- Interoperabilität der betreffenden Systeme
- Abhängigkeit von Dritten
- Einsatz nach SdT führt an anderer Stelle zum Absenken der IT-Sicherheit
- Beurteilung von Maßnahmen-Bündeln/ -Pakten zulässig

Angemessenheits-kriterien: wirtschaftlich


Herstaub/Shutterstock.com

- Quote des IT-Sicherheits-Budgets
- Letzte Investitionen
- Verhältnis zwischen Investition und Sicherheitszugewinn

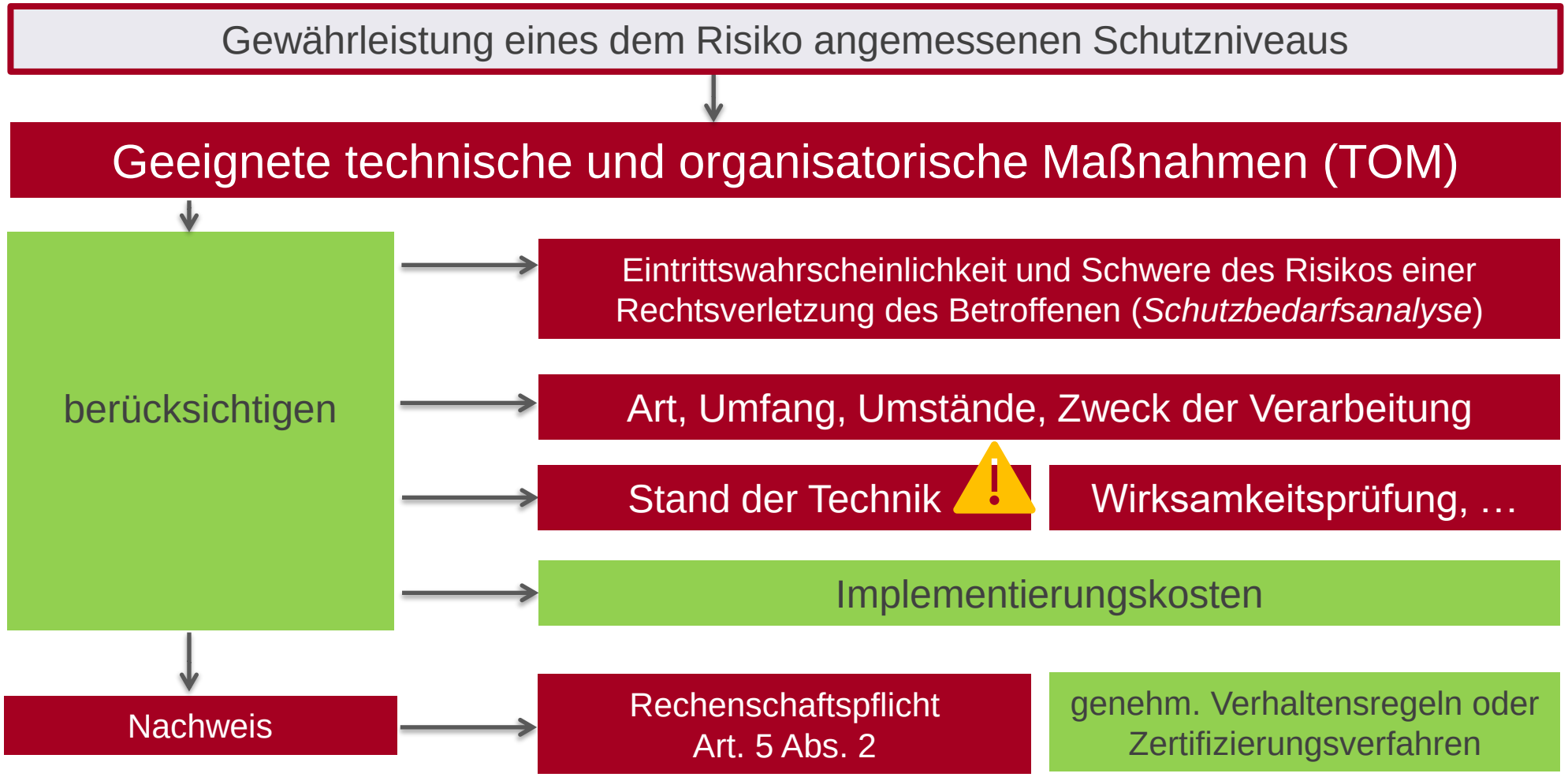
Angemessenheits-kriterien: rechtlich


Herstaub/Shutterstock.com

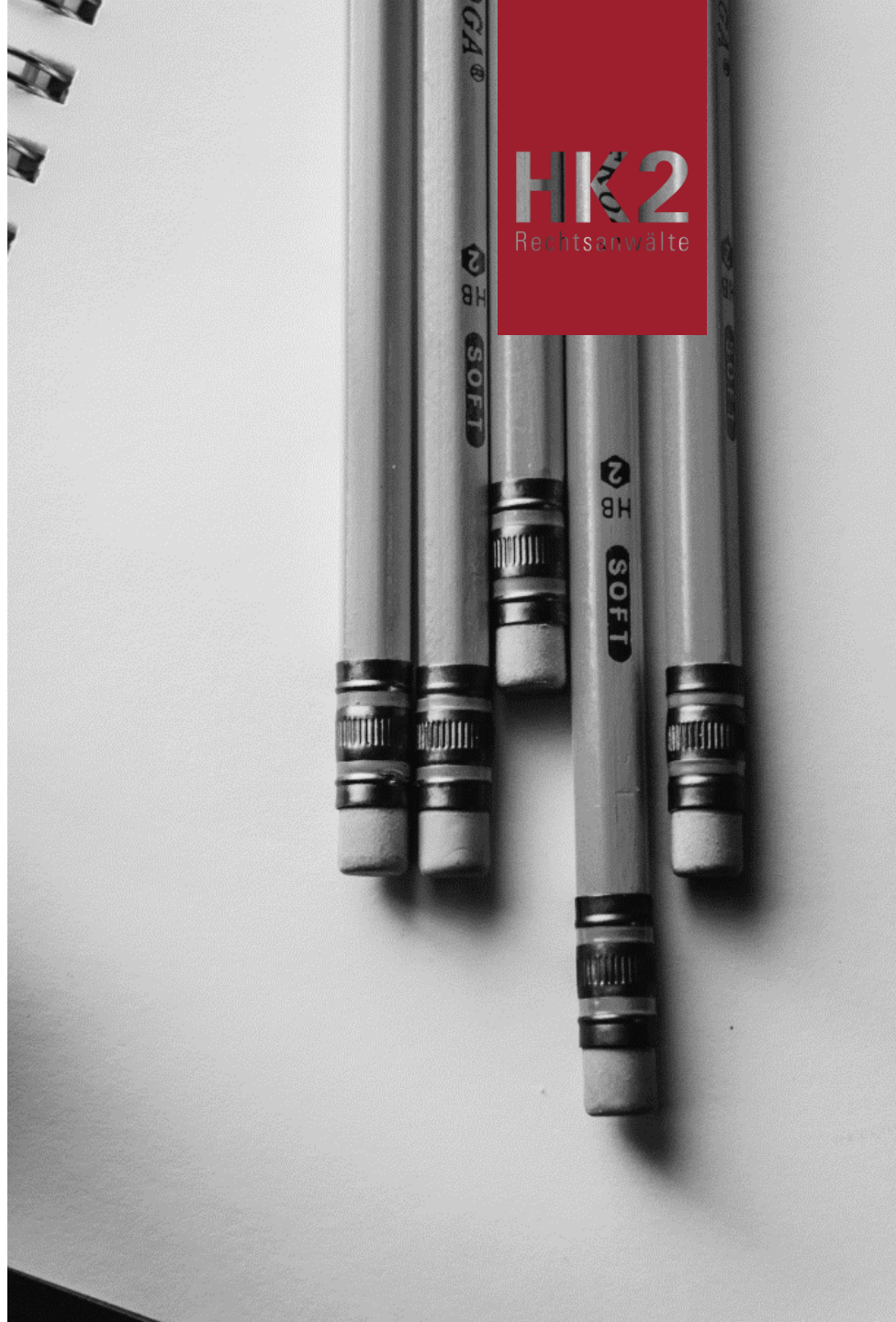
- aufsichtsrechtliche Vorgaben und Entscheidungen
- vertragliche Abhängigkeiten?

Sicherheit der Verarbeitung
Art. 32 DSGVO

HK2 Rechtsanwälte



Dokumentation
Art. 32 DSGVO



Strukturvorschlag TOM

HK2 Rechtsanwälte

BDSG (Anlage zu § 9)	Sicherheit der Datenverarbeitung, § 64 BDSG-neu	Art. 32 DSGVO
Zugangskontrolle, Zutrittskontrolle	Zugangskontrolle (Nr. 1)	Vertraulichkeit, Integrität
Zugriffskontrolle	Datenträgerkontrolle (Nr. 2), Benutzerkontrolle (Nr. 4), Zugriffskontrolle (i.e.S.) (Nr. 5), Speicherkontrolle (Nr. 3)	
Weitergabekontrolle	Übertragungskontrolle (Nr. 6) Transportkontrolle (Nr. 8)	
Eingabekontrolle	Eingabekontrolle (Nr. 7)	
	Datenintegrität (Nr. 11)	
Auftragskontrolle	Auftragskontrolle (Nr. 12)	
	Wiederherstellbarkeit (Nr. 9)	Wiederherstellbarkeit
	Zuverlässigkeit (Nr. 10)	Belastbarkeit
Verfügbarkeitskontrolle	Verfügbarkeitskontrolle (Nr. 13)	Verfügbarkeit
Trennungsgebot	Trennbarkeit (Nr. 14)	Zweckbindung, Art. 5 Abs.1 b)

Dokumentation der TOM

Maßnahmen	Beschreibung

Dokumentation der TOM (unternehmensbezogen)

Maßnahmen	Beschreibung	Stand der Technik	
		objektiv-technisch	subjektive Auswahl

HK2 Rechtsanwälte

Dokumentation der TOM (unternehmensbezogen)

Maßnahmen	Beschreibung	Stand der Technik		Schutz-bedarf
		objektiv-technisch	subjektive Auswahl	

HK2 Rechtsanwälte

Dokumentation der TOM (unternehmensbezogen)

Maßnahmen	Beschreibung	Stand der Technik		Schutz-bedarf	Wirksam keits-prüfung
		objektiv-technisch	subjektive Auswahl		

HK2 Rechtsanwälte

Dokumentation der TOM (unternehmensbezogen)

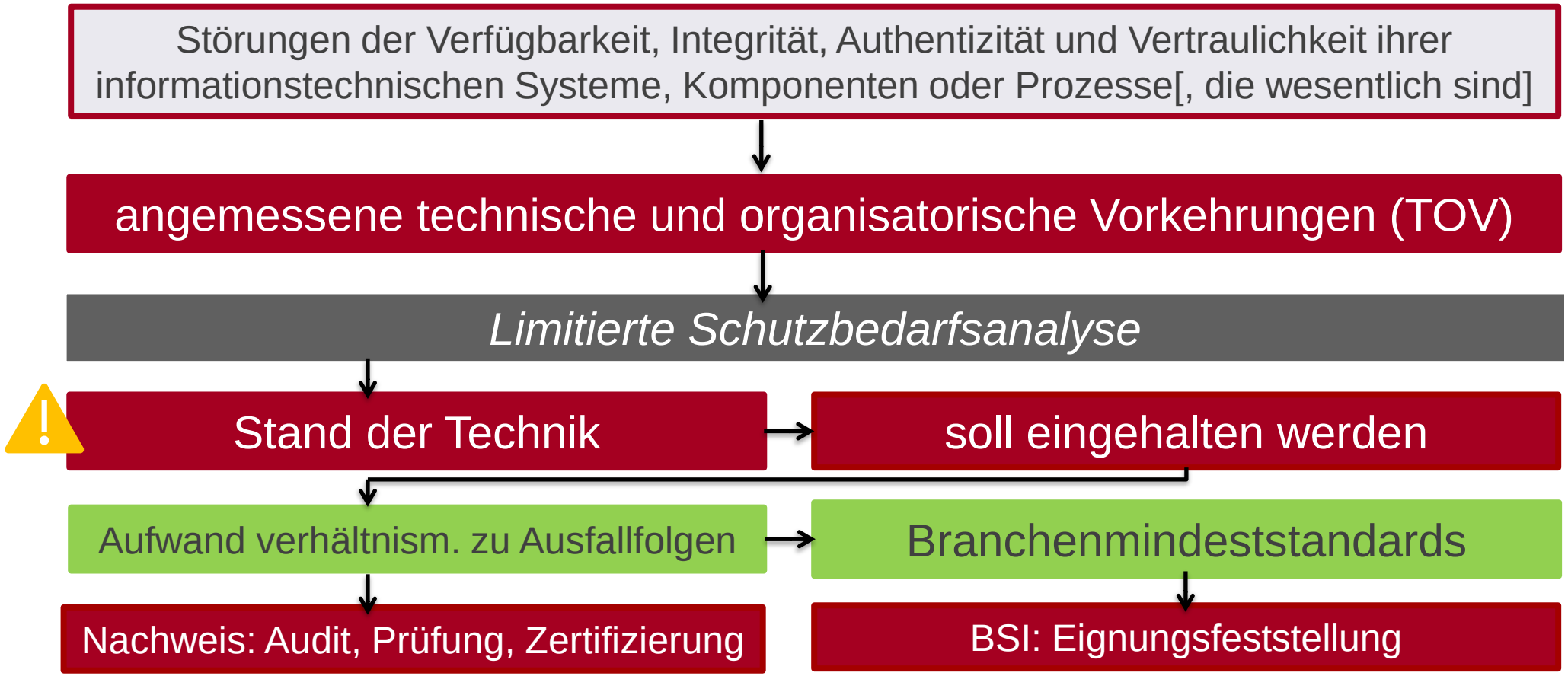
Maßnahmen	Beschreibung	Stand der Technik		Schutz-bedarf	Wirksam keits-prüfung	Wieder-vorlage	…
		objektiv-technisch	subjektive Auswahl				

HK2
Rechtsanwälte

IT-Sicherheitsgesetz

Pexels.com

§ 8a BSIG: Betreiber Kritischer Infrastrukturen sind verpflichtet, zur Vermeidung von

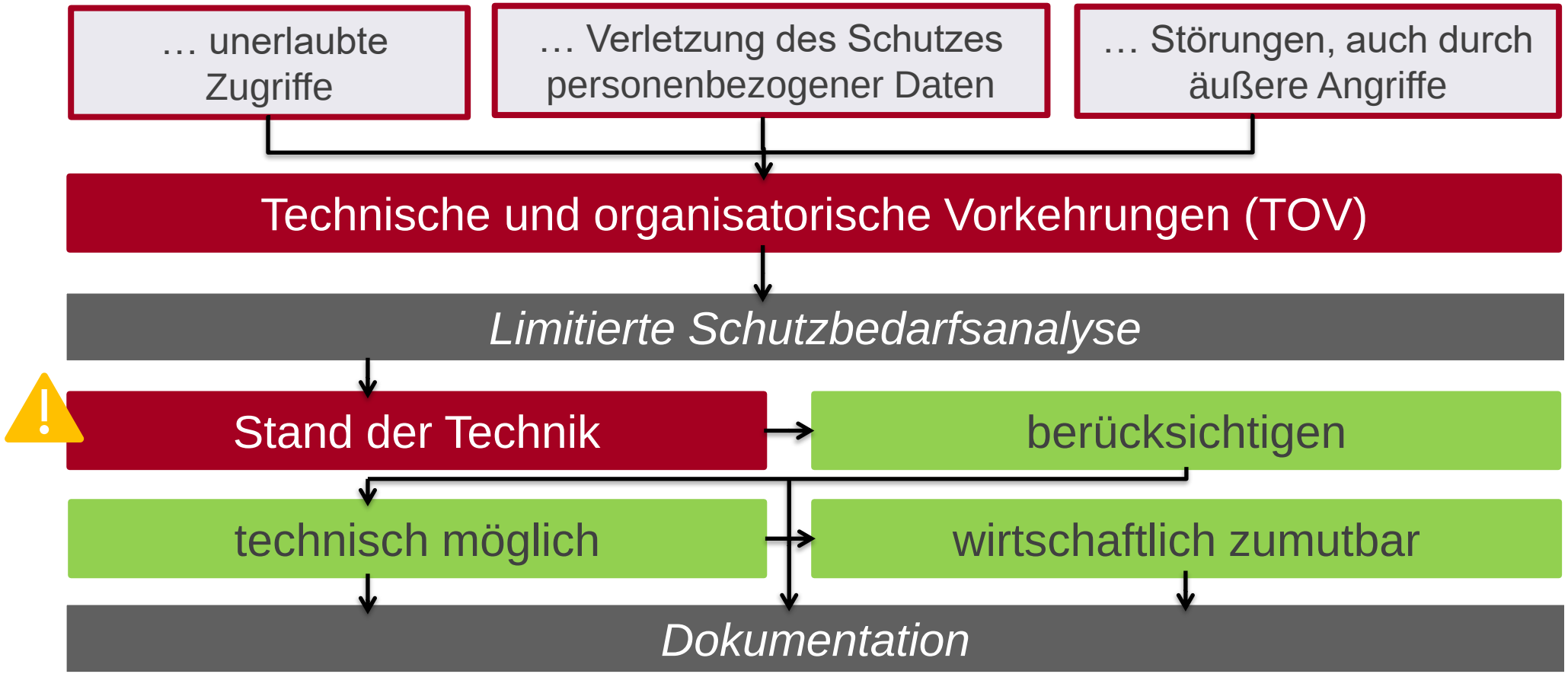


HK2
Rechtsanwälte

Telemediengesetz

Pexels.com

§ 13 Abs. 7 TMG: Sicherung der technischen Einrichtungen der Telemedienangebote gegen …

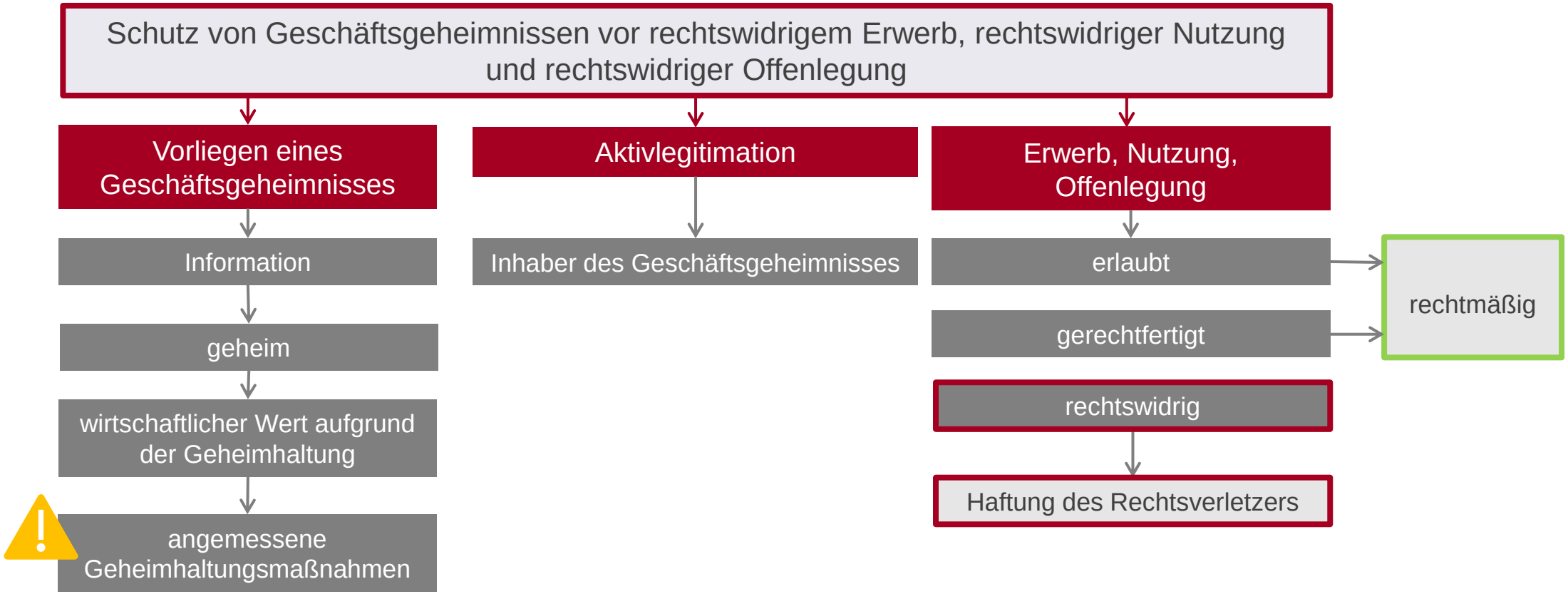


HK2
Rechtsanwälte

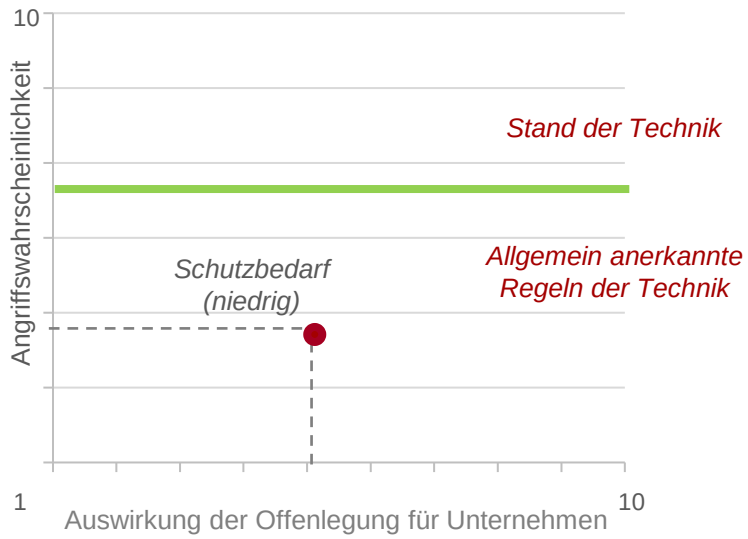
Geschäftsgeheimnisschutzgesetz

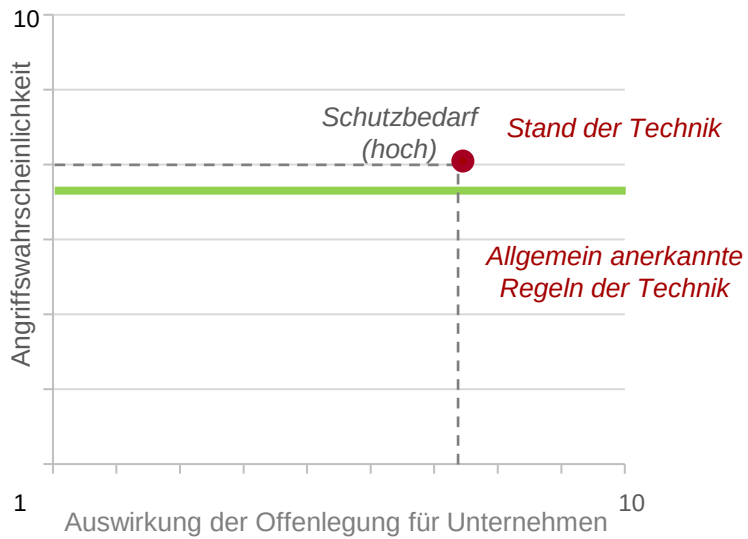
Pexels.com

Geschäftsgeheimnisschutzgesetz (GeschGehG)



Schutzbedarfsanalyse nach GeschGehG





Vertragliches

ASDF_MEDIA/Shutterstock.com

AV-Vereinbarung nach Art. 28 Abs. 3 DSGVO

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

…

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

…

AV-Vereinbarung, Anlage TOM (Sicht Anbieter)

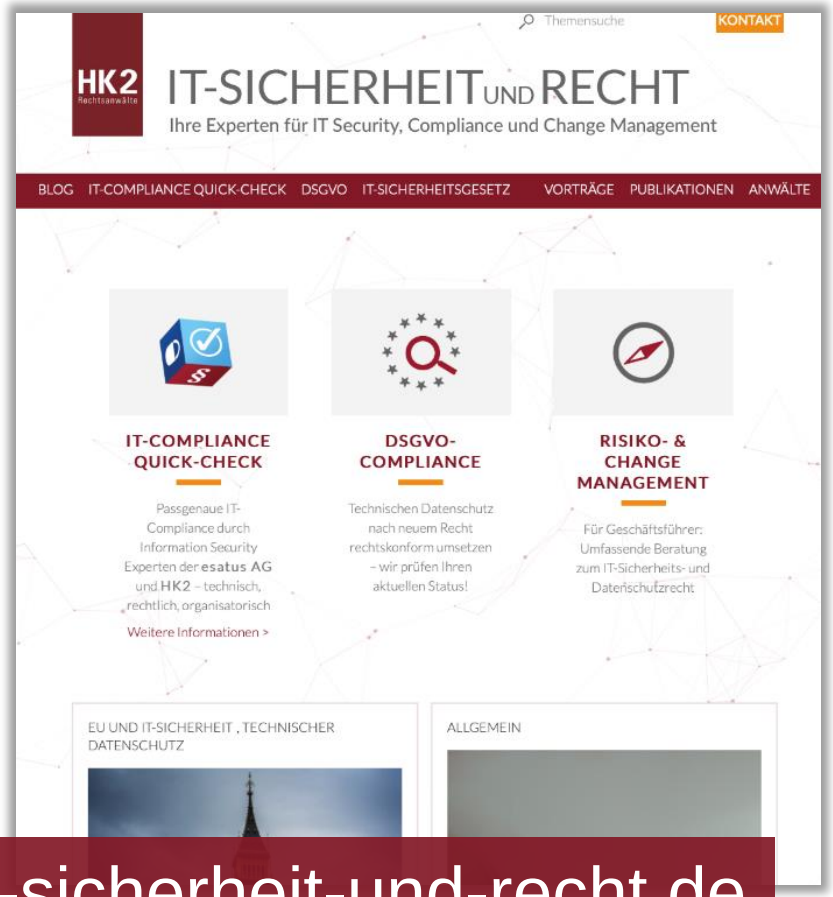
Maßnahmen	Beschreibung	Geeignetheit nach Art. 32 DSGVO

Verpflichtung zum Stand der Technik

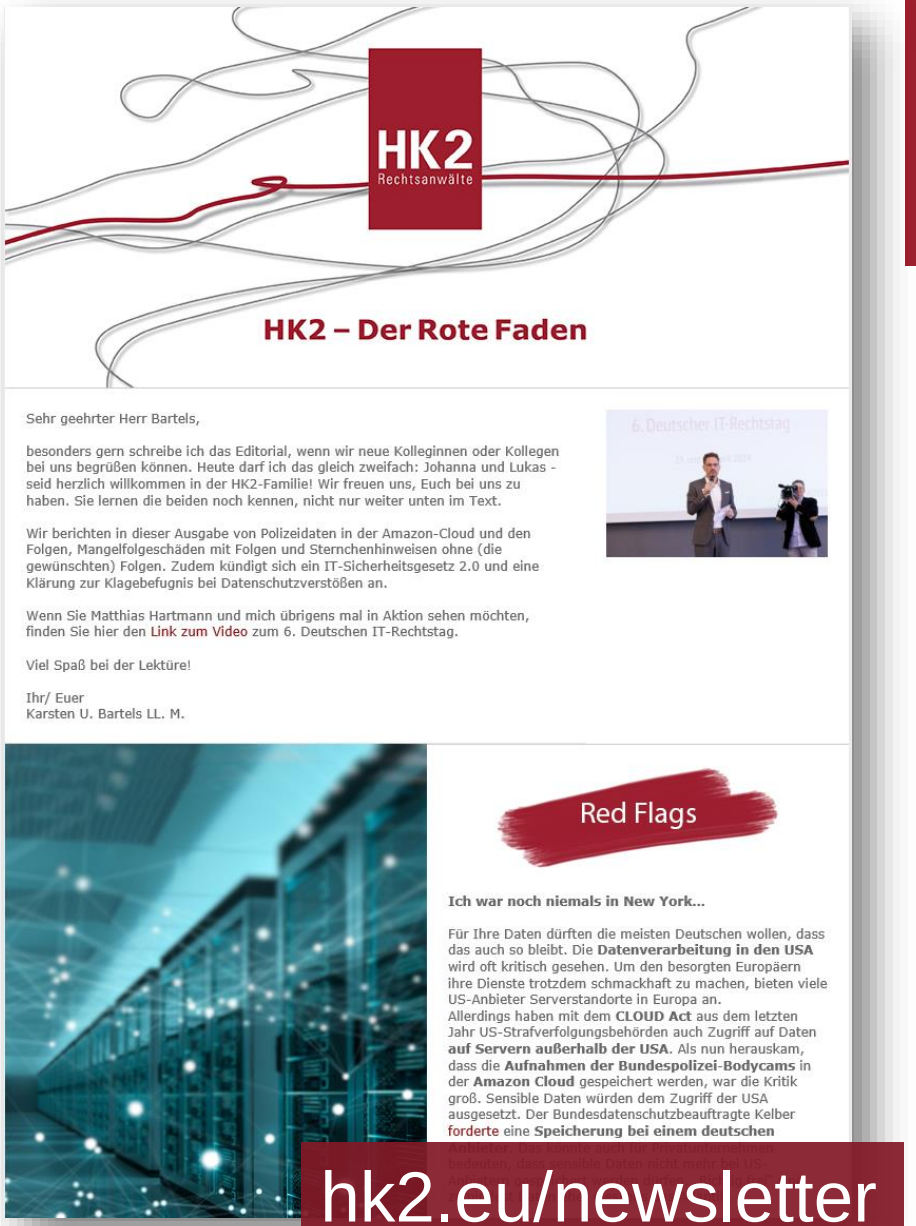
- ✓ Konkrete Verpflichtung auf den Stand der Technik
- ✓ Festlegung der Schutzmaßnahmen
  - ✓ Maßnahmenbeschreibung
  - ✓ Verknüpfung mit IT-Sicherheitszielen
- ✓ Methode
  - ✓ Nachweis zur Praxiserprobung
  - ✓ Nachweis zum Grad der Fortschrittlichkeit
  - ✓ Ggf. Standards/ Normungen und Veröffentlichungen von Fachverbänden/ Experten als Maßstab
- ✓ Dokumentation
  - ✓ Detailtiefe
  - ✓ Struktur
- ✓ Prüfung und Überprüfung
- ✓ Rechtsfolgen
- ✓ *Beachte*
  - ✓ *Perspektive AG/ AN*
  - ✓ *Angemessenheitserwägungen, planmäßiges Unterschreiten des SdT*

Auch Verträge zur IT-Sicherheit haben einen *Stand der Technik*!

HK2
Rechtsanwälte



it-sicherheit-und-recht.de



hk2.eu/newsletter

Haben Sie Fragen?

HK2
Rechtsanwälte

www.hk2.eu

www.comtection.de

HK2
Rechtsanwälte

- IT-Recht
- IP-Recht
- Arbeitsrecht

- gegründet 2002
- Wirtschaftsberatung
- Berlin - bundesweit
- www.hk2.eu

TOP WIRTSCHAFTS-KANZLEI 2019 IT & TK FOCUS DEUTSCHLANDS GROSSE KANZLEIENLISTE IN KOOPERATION MIT statista FOCUS-SPEZIAL 03 | 2019

Handelsblatt Deutschlands BESTE Anwälte 2019 HK2 Rechtsanwälte Handelsblatt · 28.06.2019 Eine Kooperation mit Best Lawyers

HK2 RECHTSANWÄLTE 2020 RECOGNIZED BY Best Lawyers

WirtschaftsWoche TOP Kanzlei IT-Recht 2019 HK2 Rechtsanwälte In Kooperation mit: Handelsblatt Research Institute Ausgabe 34/2019

Material

- Bartels u. a., Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, Bundesverband IT-Sicherheit e. V. (TeleTrusT), 2019
- Bartels/ Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214.
- Bartels/ Backer/ Schramm, Der „Stand der Technik“ im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.
- Bartels/ Schramm: Neue Anforderungen zum technischen Datenschutz nach der Datenschutz-Grundverordnung, BvD-News, 2017(1), 22-23.
- Bartels, Folgen des IT-Sicherheitsgesetzes für Telemedienanbieter – Umsetzung und Beauftragung von IT-Sicherheitsmaßnahmen nach Telemediengesetz, iX Heise, VI/ 2016.
- Bartels/ Backer, ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD, 40(1), 22.