TeleTrusT
Pioneers in IT security.

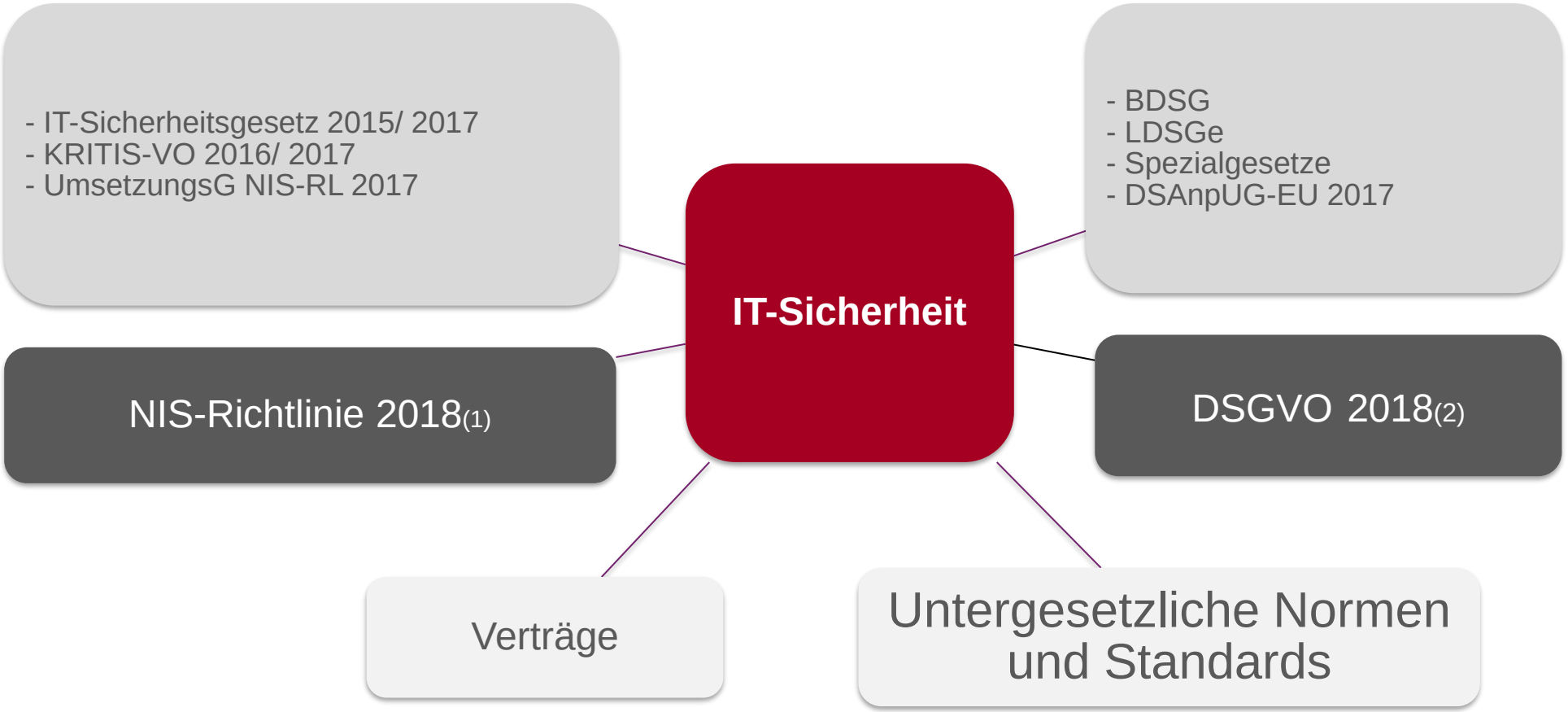
TeleTrusT-interner Workshop

Essen, 29./30.06.2017

Die Datenschutzgrundverordnung verändert alles

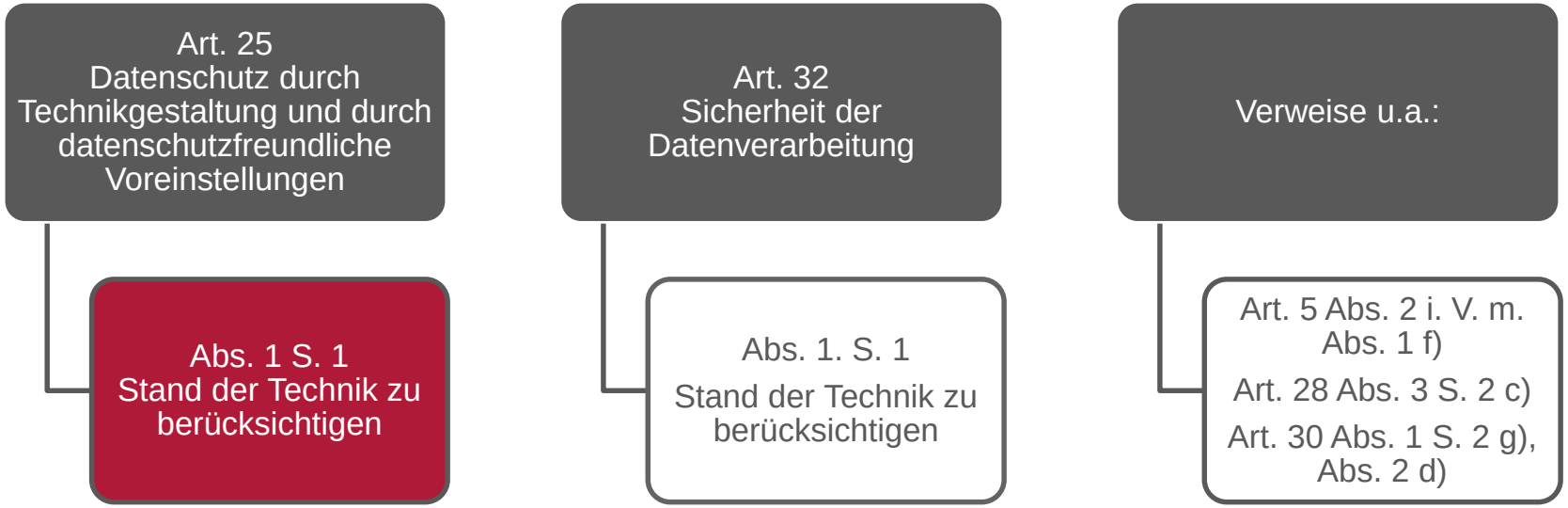
RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte



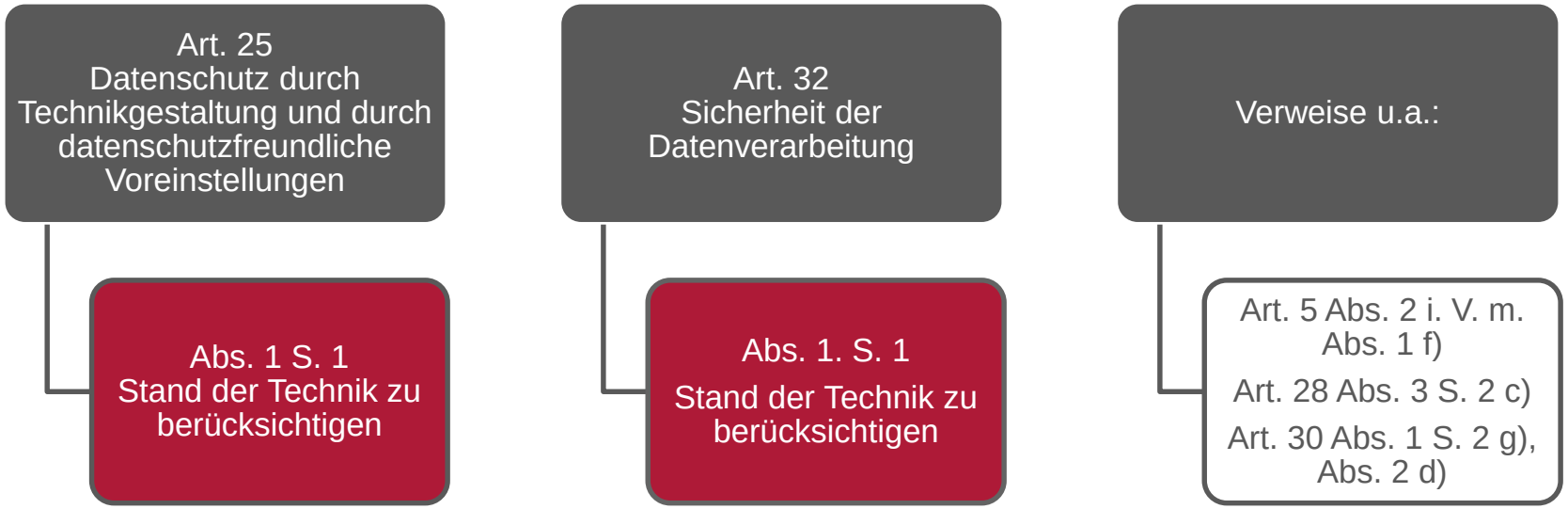
(1) Umsetzungsfristende (2) Wirksamwerden

HK2 Rechtsanwälte



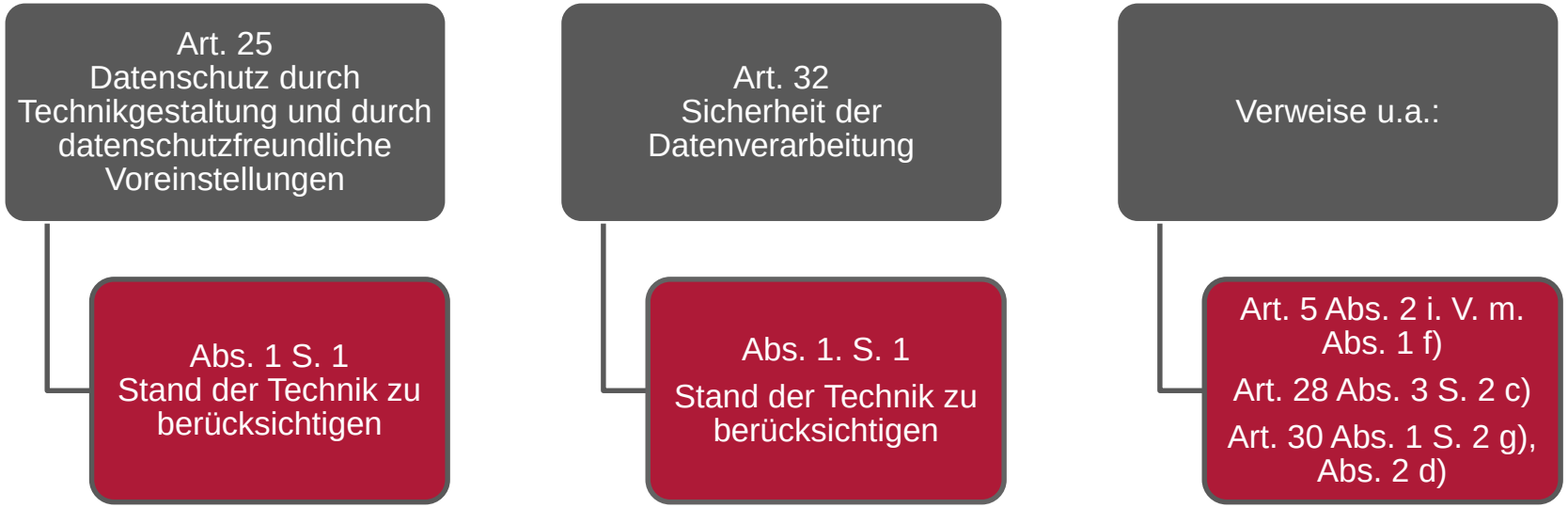
Datenschutz-Grundverordnung

HK2 Rechtsanwälte



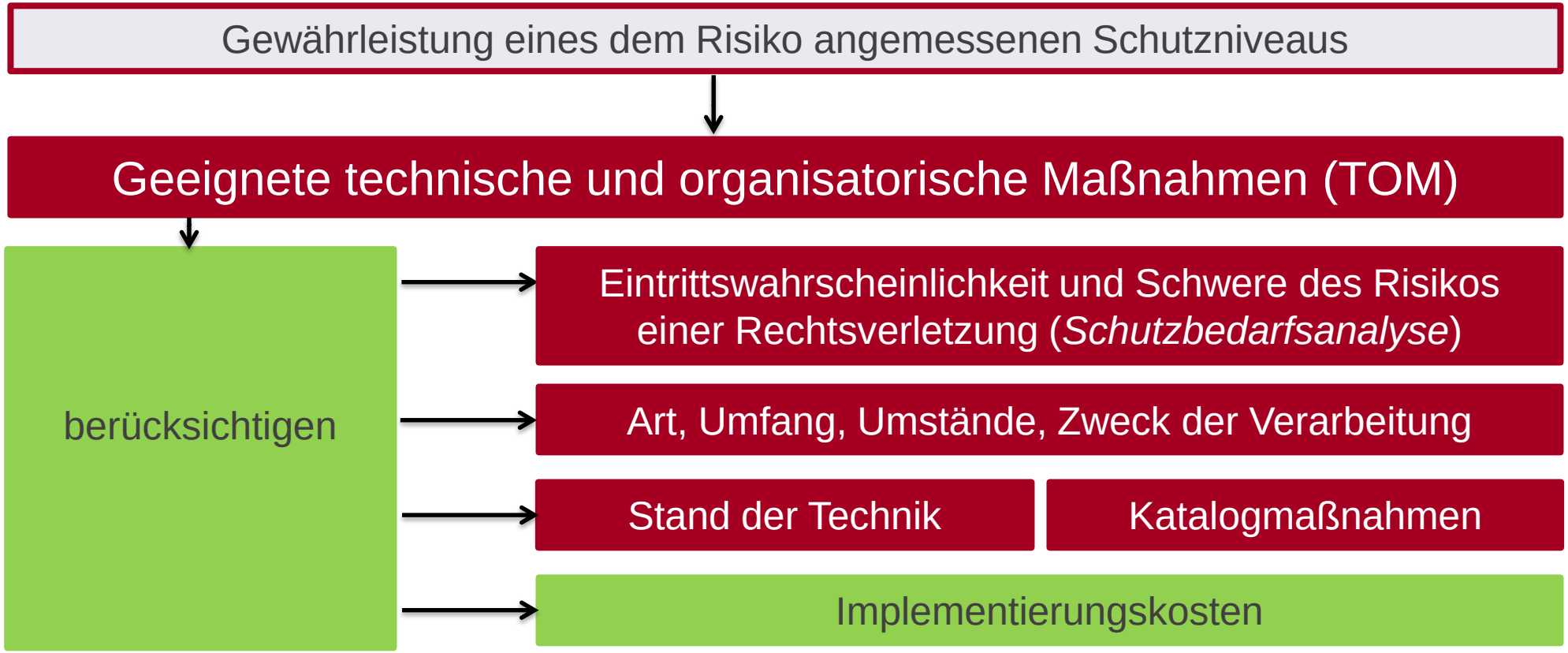
Datenschutz-Grundverordnung

HK2 Rechtsanwälte



Datenschutz-Grundverordnung

Art. 32 DSGVO: Sicherheit der Verarbeitung

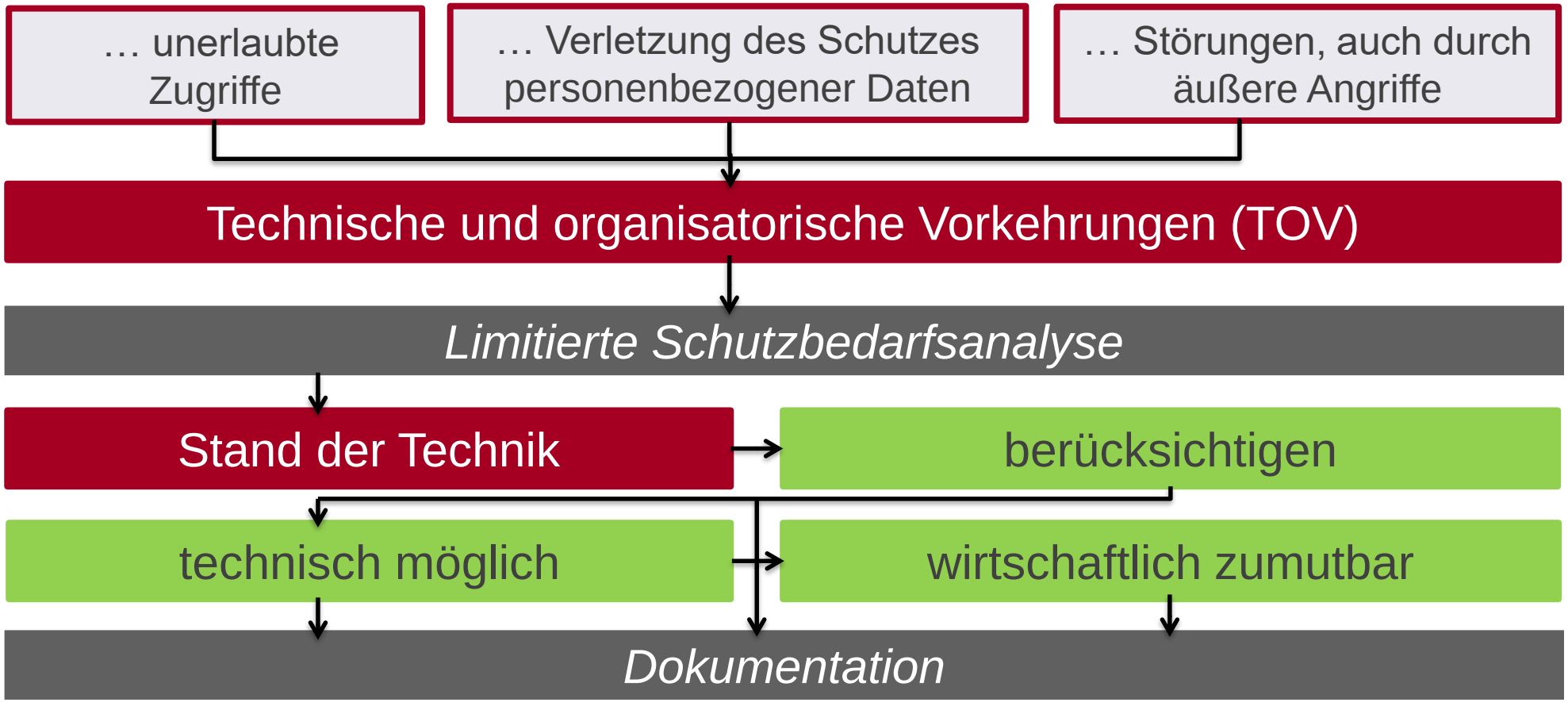


HK2
Rechtsanwälte

... zum Vergleich ...

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

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



Ermittlung des Stands der Technik

HK2 Rechtsanwälte

- Ermittlungsmethode
- Messung/ Maßstab
- Beratung/ Arbeitshilfen
- Bedeutung von technischen Normen und Richtlinien
- Prüfung
  - innerhalb/ außerhalb der Branche
  - national/ international

„Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.“
[Gesetzesbegründung zu § 8a BSIG]

HK2 Rechtsanwälte

Rechenschaftspflicht, Art. 5 DSGVO

(1) Personenbezogene Daten müssen …
… („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)
… („Zweckbindung“)
… („Datenminimierung“)
… („Richtigkeit“)
… („Speicherbegrenzung“)
… geeignete **technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“)

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen können** („**Rechenschaftspflicht**“).

Art. 28 DSGVO Auftragsverarbeitung

- Bislang „ADV“ nach § 11 BDSG
- Ab 2018: AV nach Art. 28 DSGVO
- Auftragsverarbeiter haftet direkt gegenüber Betroffenen
- Abschluss der AV-Vereinbarung auch in Textform
- Keine Beschränkung auf Datentransfer innerhalb EU/ EWR
- „TOM“ nach neuem Niveau vereinbaren (Stand der Technik)

Managen von A(D)V-Vereinbarungen

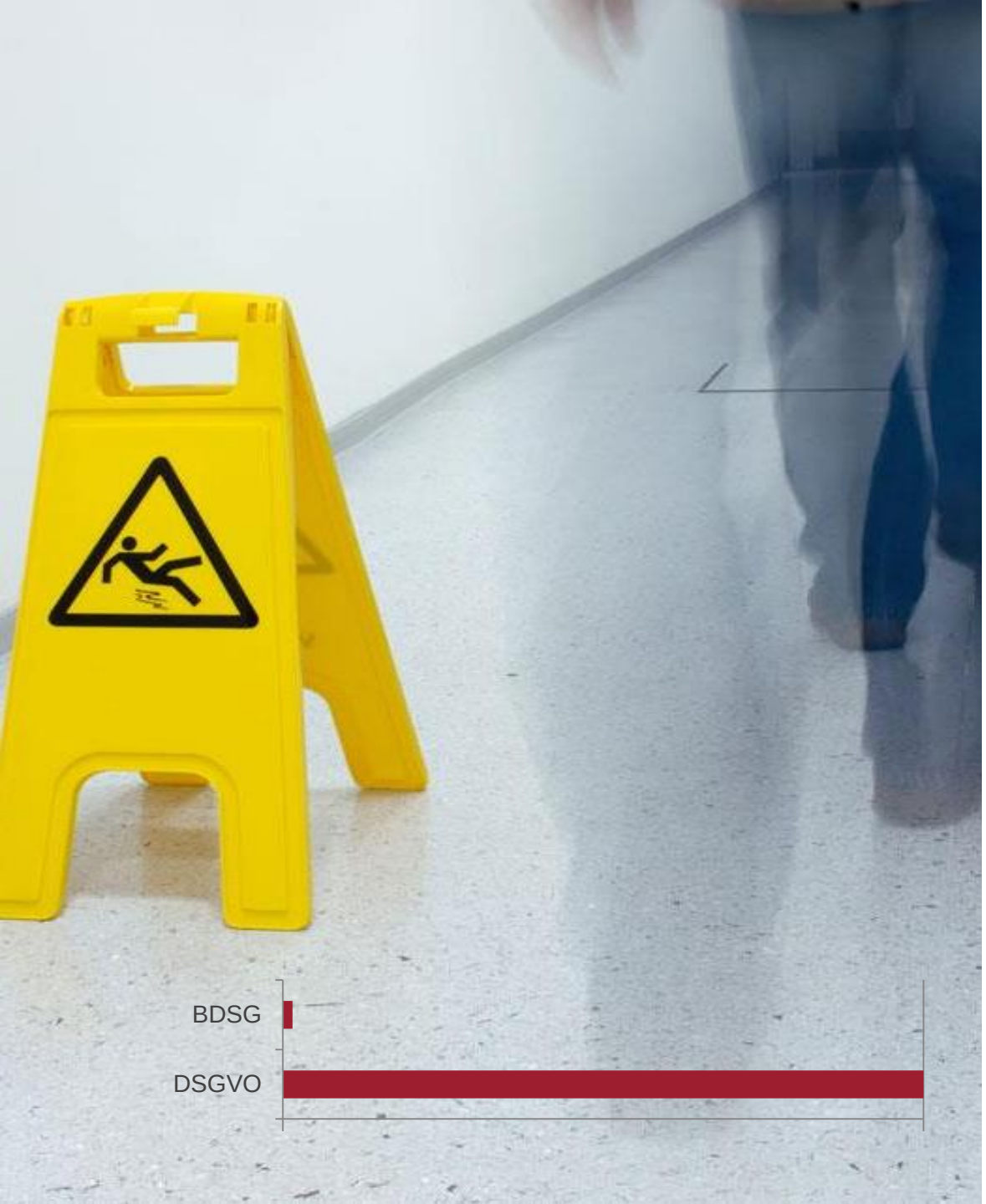
1. ADV-Vereinbarung, die bis 24.05.2018 geschlossen werden
2. AV-Vereinbarungen ab dem 25.05.2018
3. Anpassung bestehender ADV-Vereinbarungen

Lösung zu 1 + 2:

- Muster-AV-V mit DSGVO-Automatik (mit Anlage zum BDSG)

Lösung zu 3:

- Änderung der Vereinbarungen, die auf eigenem Muster basieren, projektieren
- Priorisieren, in Einheiten angehen, geplant kommunizieren



Folgen von Verstößen Art. 83

HK2 Rechtsanwälte

- Bußgelder bis EUR 20.000.000 oder 4 % des weltweiten Vorjahresumsatzes

- Beispiele
  - Verstöße i. Zshg. mit AV oder TOM: bis EUR 10 Mio. bzw. 2 % des Umsatzes
  - Verstöße gegen Rechenschaftspflicht bis EUR 20.000.000 oder 4 % des weltweiten Umsatzes

DSGVO und TeleTrusT

1. IT-Sicherheit in DSGVO vergleichbar mit ITSiG
2. Relevanz durch empfindliche Bußgelder + Reputation
3. die DSGVO ist kein Projekt
4. handhabbare Methoden anwenden
5. Anforderungen sind Verpflichteten, Zulieferern, Datenschutzbeauftragten und Aufsichtsbehörden (noch) weitgehend unbekannt