IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

Implementierung gesetzlicher IT-Sicherheitsmaßnahmen nach DSGVO und IT-Sicherheitsgesetz

RA Karsten U. Bartels LL.M.

HK2 Rechtsanwälte

Karsten U. Bartels LL.M.*

- Partner bei HK2 Rechtsanwälte
- Geschäftsführer HK2 Comtection GmbH
- Sachverständiger für IT-Produkte beim ULD S-H (rechtlich)
- Zert. Datenschutzbeauftragter (TÜV)
- Vorstand Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Stellv. Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.

*Rechtsinformatik

1. IT-Sicherheitsmaßnahmen nach DSGVO
2. Stand der Technik im Recht
3. Neue Dokumentationspflicht
4. Umstellung der Auftragsverarbeitung
5. Maßnahmen gemäß IT-Sicherheitsgesetz

HK2
Rechtsanwälte

Datenschutzgesetze

IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Verweise u. a.:

Art. 5 Abs. 1 f)

Art. 28 Abs. 3 S. 2 c)

Art. 30 Abs. 1 S. 2 g), Abs. 2 d)

IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Verweise u. a.:

Art. 5 Abs. 1 f)

Art. 28 Abs. 3 S. 2 c)

Art. 30 Abs. 1 S. 2 g), Abs. 2 d)

Sicherheit der Verarbeitung
Art. 32 DSGVO

HK2 Rechtsanwälte

Stand der Technik ist ...

… der Entwicklungsstand fortschrittlicher Verfahren, Ein-richtungen 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]

Stand der Technik

Die DSGVO darf nicht national ausgelegt werden.

HK2 Rechtsanwälte

Gegenentwurf

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

Gegenentwurf

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 **[VIVA] 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

Stand von Wissenschaft und Forschung

Stand der Technik

Allgemein anerkannte Regeln der Technik

Ermittlung des Stands der Technik

HK2 Rechtsanwälte

- Methode
- Maßstab
- Prüfung
  - innerhalb/ außerhalb der Branche
  - national/ international
- Bedeutung von technischen Normen und Richtlinien
  - BSI IT-Grundschutz
  - ISO 27001 u. a.

Stand der Technik

objektiv-technische Ermittlung

vs.

subjektive Angemessenheit

Zulässiges Unterschreiten des Stands der Technik

Fachlich-valide Auseinandersetzung anhand von

- technischen
- wirtschaftlichen
- rechtlichen

Faktoren.

Ergebnis ist zu dokumentieren, Art. 5 Abs. 2 DSGVO.

HK2
Rechtsanwälte

it-sa 2017 | TeleTrusT

TeleTrusT
Pioneers in IT security.

Unterschreiten des Stands der Technik in der IT-Sicherheit

Dieser Beitrag beleuchtet zulässige Handlungsoptionen und Rechtsfolgen von Fehlentscheidungen im Zusammenhang mit der EU-Datenschutz-Grundverordnung (DS-GVO), der europäischen Netzwerk- und Informationssicherheits-(NIS-)Richtlinie sowie dem deutschen IT-Sicherheitsgesetz.

Von Karsten U. Bartels LL.M., HK2 Rechtsanwälte Berlin – Vorstand Bundesverband IT-Sicherheit e. V. (TeleTrusT)

In den letzten Monaten wurden zahlreiche Gesetze verabschiedet, die das Niveau der IT-Sicherheit erhöhen sollen. Dazu gehören das IT-Sicherheitsgesetz (ITSiG), die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) sowie die ab Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO).

Das zentrale Tatbestandsmerkmal für die IT-Sicherheit dieser Normen ist der „Stand der Technik". Damit dieser objektiv-technische Begriff durch die Verpflichteten in der Praxis umgesetzt werden kann, enthalten die jeweiligen Datenverarbeitung ist der Art. 32 DS-GVO: Diese Norm sieht vor, dass Verantwortliche unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Auch das IT-Sicherheitsgesetz sieht Maßnahmen nach dem Stand der Technik für Betreiber so genannter kritischer Infrastrukturen vor (§ 8a BSIG). KRITIS-Betreiber sind verpflichtet, zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT angemessene organisatorische und technische

<kes> Die Zeitschrift für Informations-Sicherheit, 2017, Ausgabe 5

Dokumentation
Art. 32 DSGVO

Dokumentation der TOM

Maßnahmen	Beschreibung

Dokumentation der TOM

Maßnahmen	Beschreibung	Stand der Technik	
		objektiv-technisch	subjektive Auswahl

Dokumentation der TOM

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

Dokumentation der TOM

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

Dokumentation der TOM

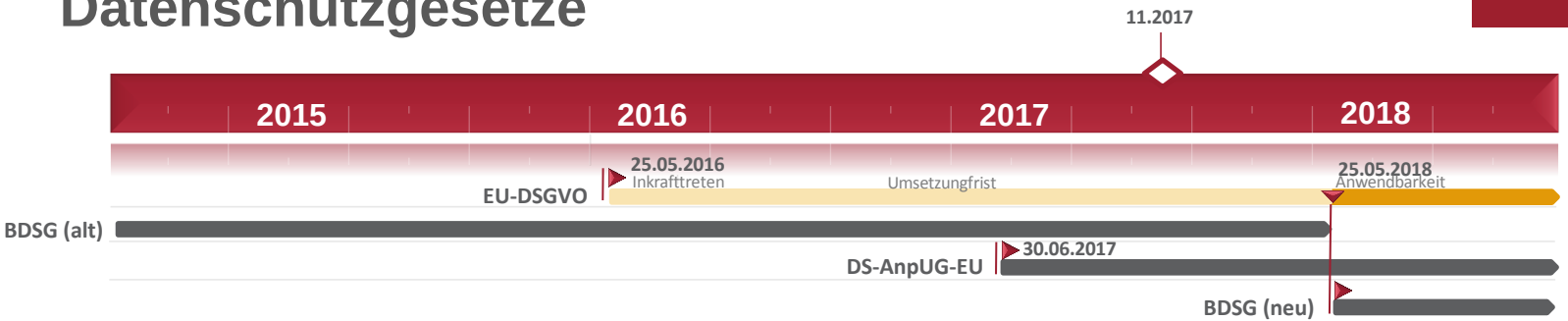
Maßnahmen	Beschreibung	Stand der Technik		Schutz-bedarf	Wirksam keits-prüfung	Wieder-vorlage	…
		objektiv-technisch	subjektive Auswahl				

HK2
Rechtsanwälte

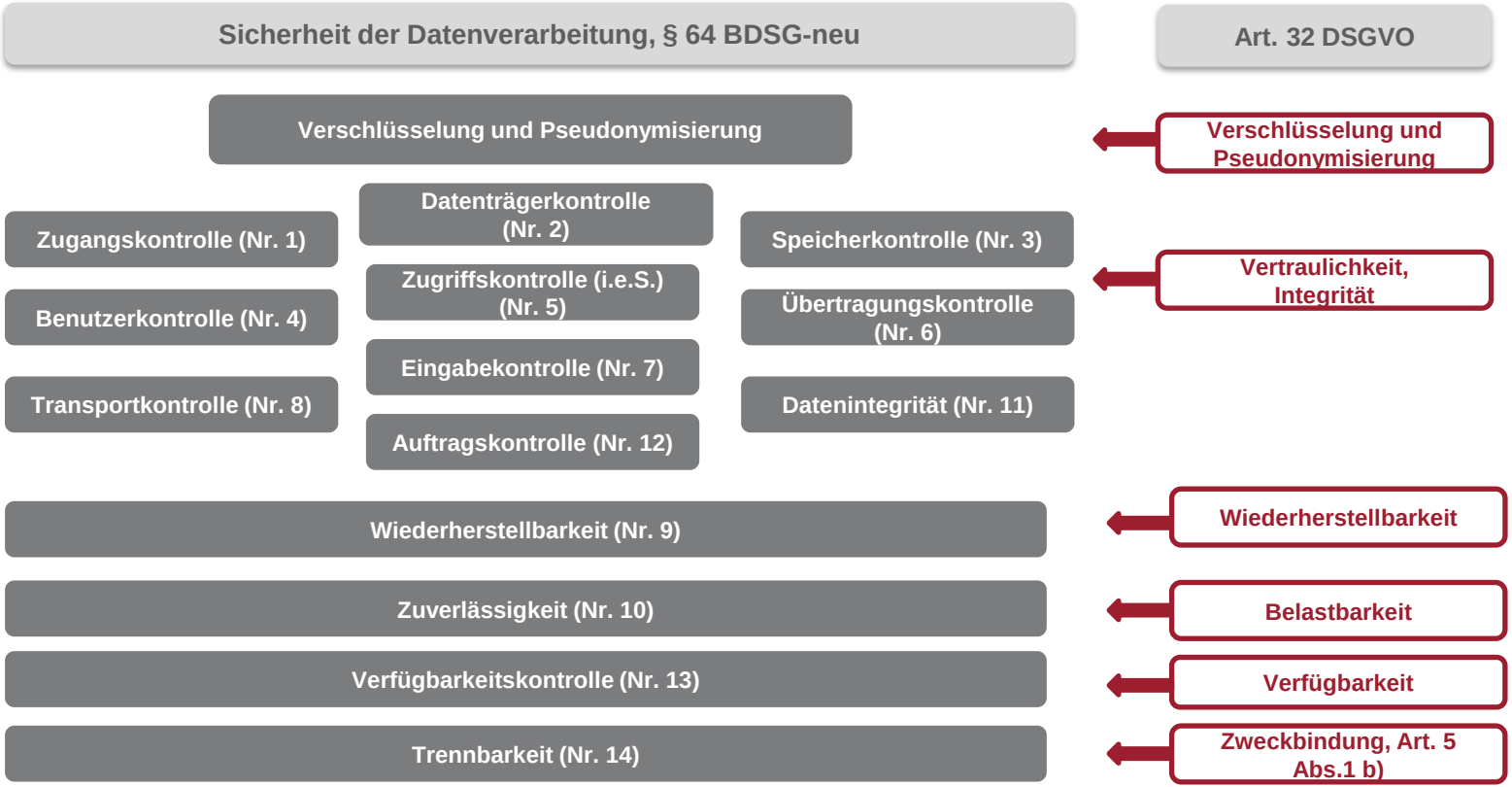
Datenschutzgesetze

HK2
Rechtsanwälte

Datenschutzgesetze



HK2 Rechtsanwälte



IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Verweise u. a.:

Art. 5 Abs. 1 f)

Art. 28 Abs. 3 S. 2 c)

Art. 30 Abs. 1 S. 2 g), Abs. 2 d)

IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Verweise u. a.:

Art. 5 Abs. 1 f)

Art. 28 Abs. 3 S. 2 c)

Art. 30 Abs. 1 S. 2 g), Abs. 2 d)

Data protection by design and by default Art. 25 DSGVO

HK2 Rechtsanwälte

- geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik
- Adressat ist der Verantwortliche
- entspricht teilw. Datenvermeidung und Datensparsamkeit
- Abs. 1 - by Design
  Umsetzung der Datenminimierung ist durch technische und organisatorische Mittel sicherzustellen
- Abs. 2 - by Default
  Datenverarbeitungsprozesse müssen so voreingestellt sein, dass nur die erforderlichen Daten erhoben werden

IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Verweise u. a.:

Art. 5 Abs. 1 f)

Art. 28 Abs. 3 S. 2 c)

Art. 30 Abs. 1 S. 2 g), Abs. 2 d)

IT-Sicherheit in der Datenschutz-Grundverordnung

HK2 Rechtsanwälte

Art. 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 32
Sicherheit der Datenverarbeitung

Art. 28 Abs. 3 S. 2 c)
i. V. m. Art. 32

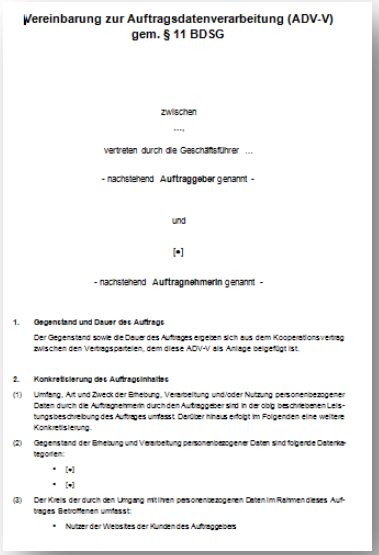
Auftragsverarbeitung (AV) Art. 28 DSGVO

- AV-Vereinbarung (bislang ADV)
- Auftragsverarbeiter haftet direkt gegenüber Betroffenen (Art. 82 DSGVO)
- Auftragsverarbeiter hat alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zu treffen
- Pflicht des Auftraggebers zur sorgfältigen Auswahl des Auftragsverarbeiters (Art. 28 Abs. 1 DSGVO)
- keine Beschränkung auf Datentransfer innerhalb EU/ EWR

bisher
Auftragsdatenverarbeitung

HK2 Rechtsanwälte

§ 11 BDSG



Vereinbarung zur Auftragsdatenverarbeitung (ADV-V) gem. § 11 BDSG

zwischen

---

vertreten durch die Geschäftsführer ...

- nachstehend **Auftraggeber** genannt -

und

[•]

- nachstehend **Auftragnehmerin** genannt -

1. **Gegenstand und Dauer des Auftrags**

Der Gegenstand sowie die Dauer des Auftrages ergeben sich aus dem Kooperationsvertrag zwischen den Vertragsparteien, dem diese ADV-V als Anlage beigefügt ist.

2. **Konkretisierung des Auftragsinhaltes**

(1) Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch die Auftragnehmerin durch den Auftraggeber sind in der oben beschriebenen Leistungsbeschreibung des Auftrages umfasst. Darüber hinaus erfolgt im Folgenden eine weitere Konkretisierung.

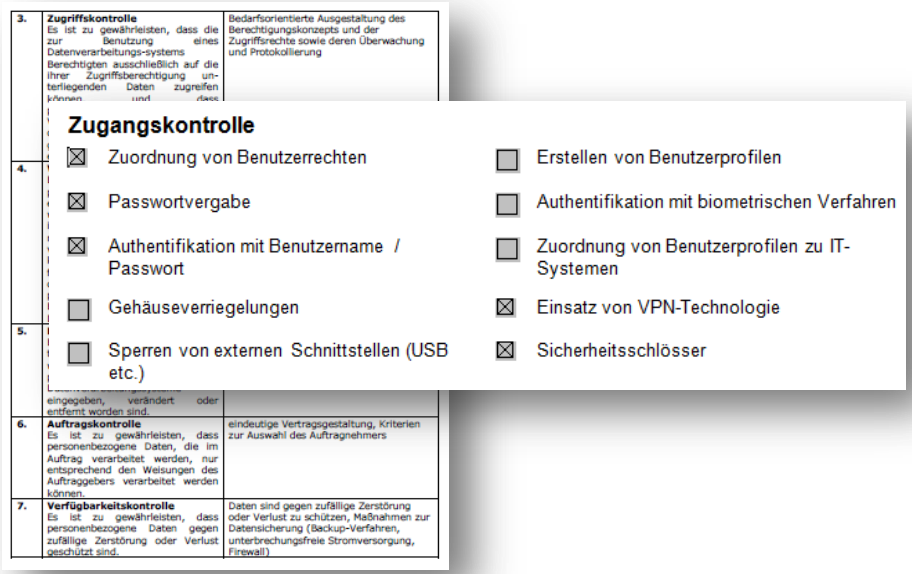
(2) Gegenstand der Erhebung und Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- [•]
- [•]

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrages Betroffenen umfasst:

- Nutzer der Websites der Kunden des Auftraggebers

§ 9 Satz 1 BDSG i. V. m. Anlage zum BDSG



3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass	Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung
4.		
5.	eingegeben, verändert oder entfernt worden sind.	
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragnehmers
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Backup-Verfahren, unterbrechungsfreie Stromversorgung, Firewall)

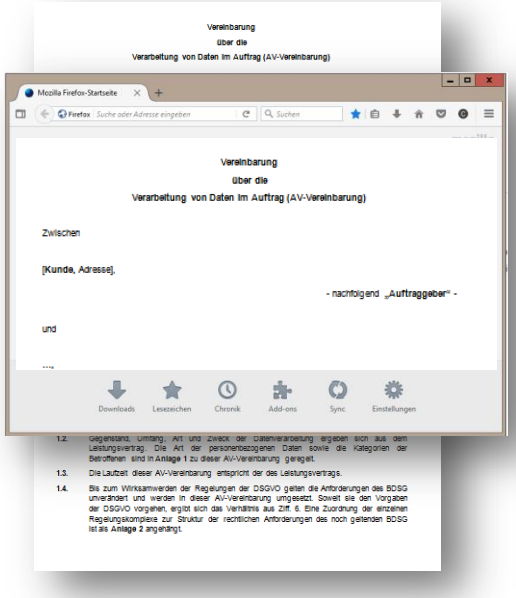
Zugangskontrolle

☒ Zuordnung von Benutzerrechten	☐ Erstellen von Benutzerprofilen
☒ Passwortvergabe	☐ Authentifikation mit biometrischen Verfahren
☒ Authentifikation mit Benutzername / Passwort	☐ Zuordnung von Benutzerprofilen zu IT-Systemen
☐ Gehäuseverriegelungen	☒ Einsatz von VPN-Technologie
☐ Sperren von externen Schnittstellen (USB etc.)	☒ Sicherheitsschlösser

Ab 25.05.2018
Auftragsverarbeitung

HK2 Rechtsanwälte

Art. 28 DSGVO



Art. 28 Abs. 3 c) i. V. m. Art. 32 DSGVO

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

Maßnahmen	Beschreibung	Geeignetheit nach Art. 32 DSGVO

Umstellungsprojekt: A(D)V-Vereinbarungen

Verwendung	**bis 24.05.2018 Neuverträge**
Verantwortlicher als AN	1. Muster-AV-Vereinbarung mit DSGVO-Automatik
Verantwortlicher als AG	2. Muster-AV-Vereinbarung mit DSGVO-Automatik

Umstellungsprojekt: A(D)V-Vereinbarungen

Verwendung	**bis 24.05.2018 Neuverträge**	**bis 24.05.2018 Änderung Bestandsverträge**
Verantwortlicher als AN	1. Muster-AV-Vereinbarung mit DSGVO-Automatik	3. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018
Verantwortlicher als AG	2. Muster-AV-Vereinbarung mit DSGVO-Automatik	4. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018

HK2 Rechtsanwälte

Umstellungsprojekt: A(D)V-Vereinbarungen

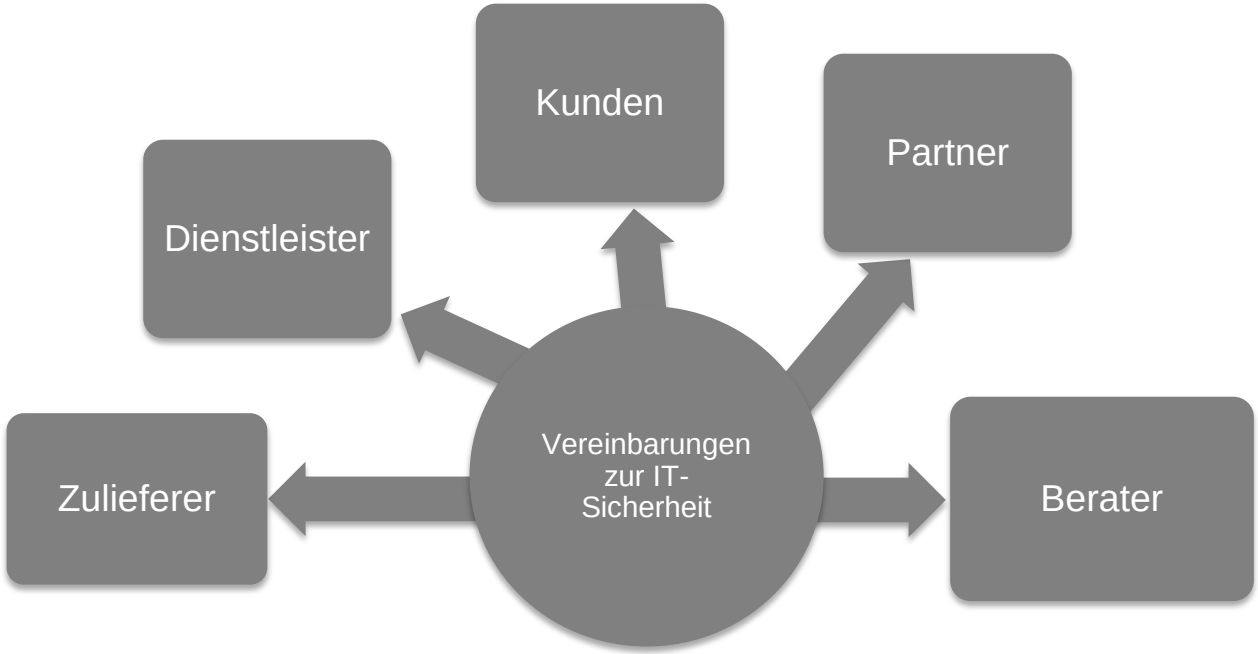
Verwendung	**bis 24.05.2018 Neuverträge**	**bis 24.05.2018 Änderung Bestandsverträge**	**ab 25.05.2018**
Verantwortlicher als AN	1. Muster-AV-Vereinbarung mit DSGVO-Automatik	3. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018	5. Muster-AV-Vereinbarung (nur DSGVO)
Verantwortlicher als AG	2. Muster-AV-Vereinbarung mit DSGVO-Automatik	4. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018	6. Muster-AV-Vereinbarung (nur DSGVO)

Umstellungsprojekt: A(D)V-Vereinbarungen

Verwendung	**bis 24.05.2018 Neuverträge**	**bis 24.05.2018 Änderung Bestandsverträge**	**ab 25.05.2018**	***Unterschied***
Verantwortlicher als AN	1. Muster-AV-Vereinbarung mit DSGVO-Automatik	3. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018	5. Muster-AV-Vereinbarung (nur DSGVO)	*mit Haftungs-klausel und Freistellung*
Verantwortlicher als AG	2. Muster-AV-Vereinbarung mit DSGVO-Automatik	4. Muster-AV-Vereinbarung, aufschiebend bedingt bis zum 25.05.2018	6. Muster-AV-Vereinbarung (nur DSGVO)	

HK2
Rechtsanwälte

Verträge mit Bezügen zur IT-Sicherheit



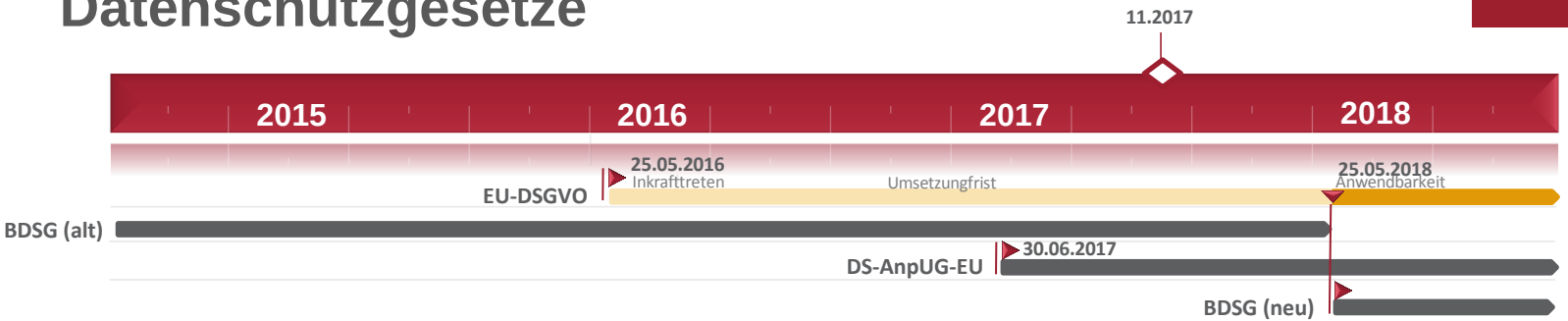
Anpassung von Verträgen mit Bezügen zu Datenschutz/ IT-Sicherheit

HK2 Rechtsanwälte

- Beispiele
  - Produktbeschreibungen
  - Technische Feinspezifikationen
  - Lasten-/ Pflichtenhefte
  - A(D)V-Vereinbarungen
  - Support-Verträge/ SLAs
  - Vertragsanlagen IT-Sicherheit oder Datenschutz
  - Datenschutzkonzepte
  - IT-Sicherheitskonzepte

HK2
Rechtsanwälte

Datenschutzgesetze



HK2
Rechtsanwälte

Datenschutz- und IT-Sicherheitsgesetze

IT-Sicherheitsmaßnahmen der IT-Sicherheitsgesetze

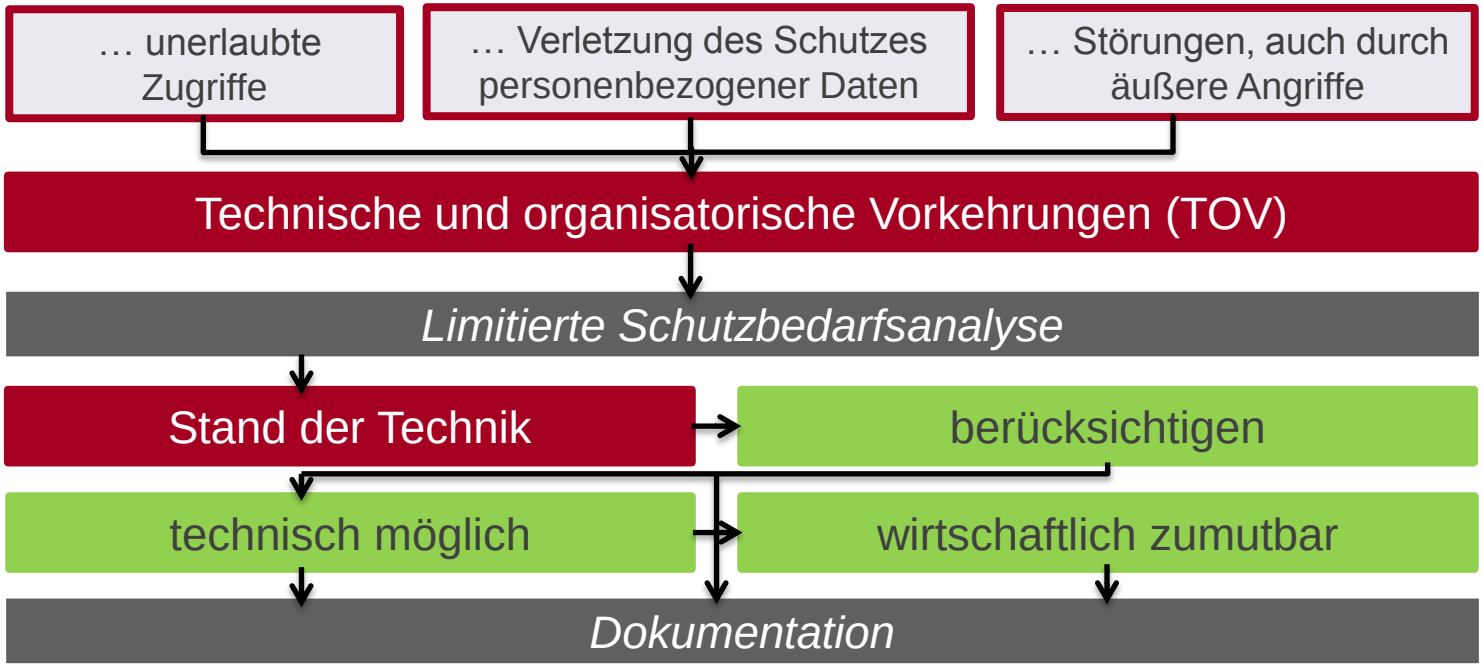
- **§ 8a BSIG (KRITIS)**
- § 8c BSIG (Anbieter digitaler Dienste)
- § 13 Abs. 7 TMG (Online-Dienste)
- § 109 TKG
- § 11 Abs. 1a ff. EnWG
- […]

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

IT-Sicherheitsmaßnahmen der IT-Sicherheitsgesetze

- § 8a BSIG (KRITIS)
- § 8c BSIG (Anbieter digitaler Dienste)
- **§ 13 Abs. 7 TMG (Online-Dienste)**
- § 109 TKG
- § 11 Abs. 1a ff. EnWG
- […]

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



Thesen zum technischen Datenschutz der DSGVO

HK2 Rechtsanwälte

1. Der technische Datenschutz erreicht das Niveau der IT-Sicherheitsgesetze.
2. Die Verpflichtung auf den Stand der Technik wird universell.
3. Stand der Technik: Comply or explain!
4. Aus Listen werden Dokumentationen.
5. IT-Sicherheit ist (fast) immer vertraglich zu vereinbaren.
6. Auslegungsspielräume der DSGVO sind historisch groß, aber degressiv.

Haben Sie Fragen?

HK2
Rechtsanwälte

www.it-sicherheit-und-recht.de

www.hk2.eu/newsletter