Security by Design – Technischer Datenschutz in der Datenschutz-Grundverordnung

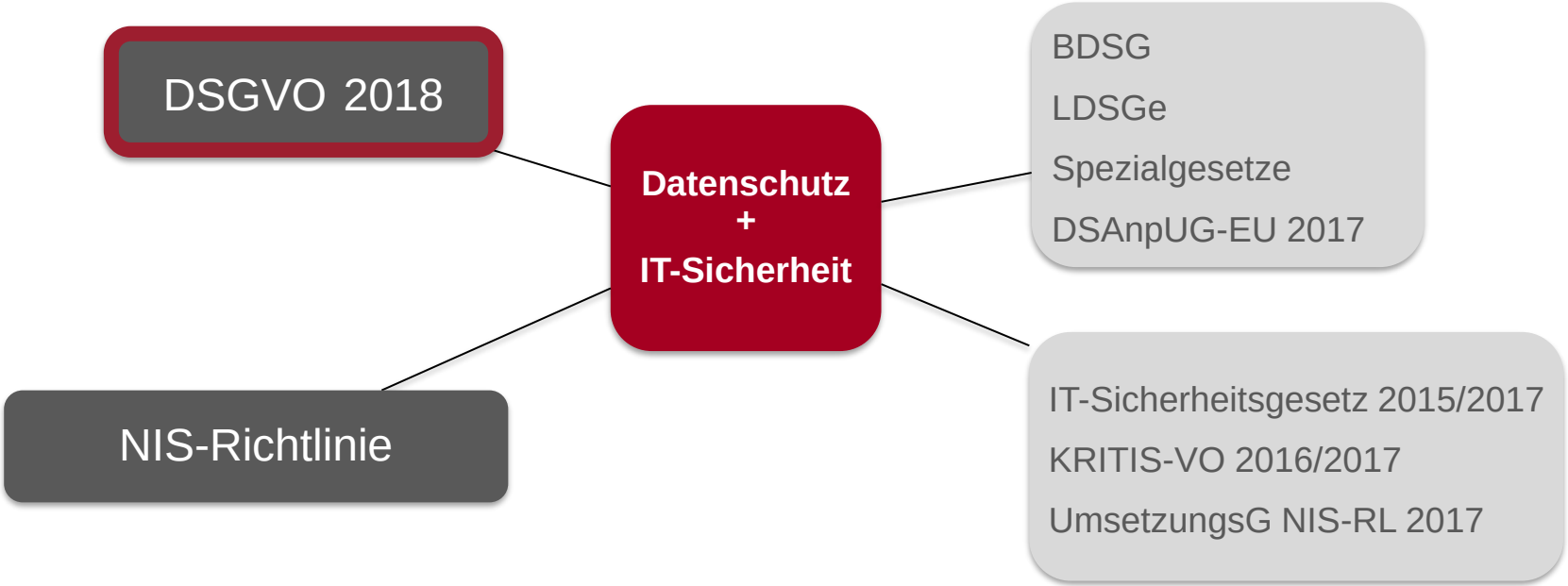
Merlin Backer LL.M. (Glasgow) | HK2 Rechtsanwälte
eco Internet Security Days 2017, 28.09.2017

1 Gesetzliche Grundlagen
2 IT-Sicherheitsgesetz
3 Datenschutz-Grundverordnung
- Datenschutzprinzipien
- Neue Pflichten
- TOM

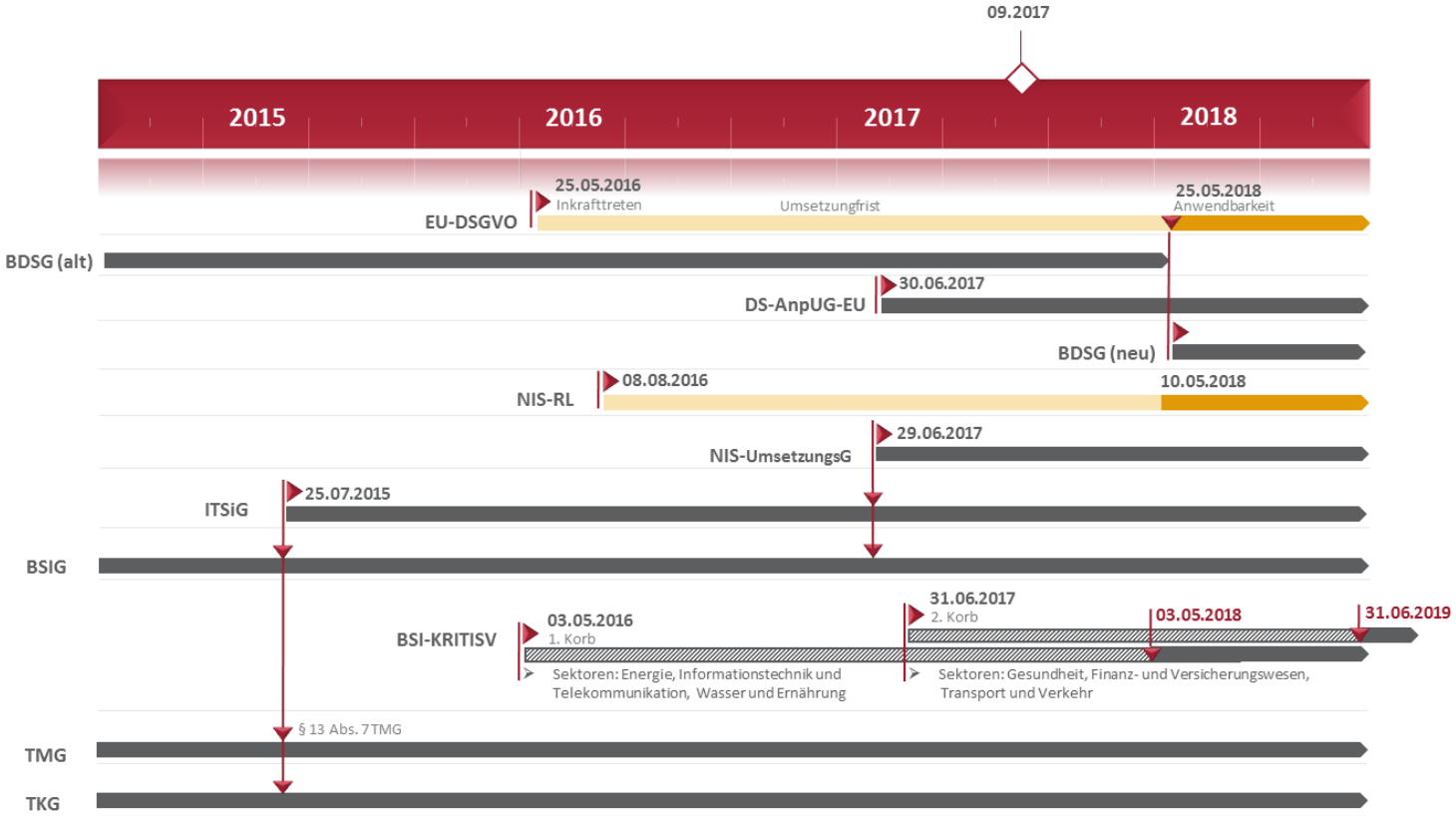
4 Konkreter Umsetzungsbedarf
- Dokumentationspflichten
- Vertragsgestaltung

HK2 Rechtsanwälte

Stand der Gesetzgebung



HK2
Rechtsanwälte



IT-Sicherheitsgesetz (ITSiG)

HK2 Rechtsanwälte

BSIG Art. 1

AtomG Art. 2

EnWiG Art. 3

TMG Art. 4

TKG Art. 5

Art. 6-10

Die Datenschutz-Grundverordnung

- Die DSGVO wurde im Mai 2016 im Gesetzblatt verabschiedet
- Gültigkeit der Regelungen nach zweijähriger Übergangsfrist ab **25.05.2018**
- DSGVO schafft ein einheitliches Datenschutzrecht in ganz Europa
- Führt zur Vollharmonisierung, enthält aber sog. „Öffnungsklauseln“
- Wirkt unmittelbar und löst nationales Datenschutzrecht, wie das BDSG, ab
- BDSG wird angepasst und enthält Öffnungsregeln
- Verpflichtet Unternehmen und die öffentliche Verwaltung gleichermaßen

Datenschutzprinzipien, Art. 5 & 25 DSGVO

HK2 Rechtsanwälte

Folgen von Verstößen, Art. 83 DSGVO

- DSGVO erhöht Bußgelder im Vergleich zu BDSG massiv

- § 43 BDSG: Bußgelder bis max. EUR 300.000
- Art. 83 DSGVO: Bußgelder bis EUR 20.000.000 oder 4 % des weltweiten Vorjahresumsatzes

Haftung der Geschäftsführer

- Die Geschäftsleitung ist verantwortlich für die Organisation des Unternehmens. Bei Verletzung der Pflicht ist die Geschäftsleitung dem Unternehmen zum Ersatz der daraus resultierenden Schäden verpflichtet
  = **Schadensersatz**

- Es sind geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.
  = **Risikomanagement**

- **Datenschutz = Teil vom Risikomanagement**

Technische und organisatorische Maßnahmen

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

Technische und organisatorische Maßnahmen

- Keine Vorgabe von Maßnahmenkategorien wie in § 9 BDSG und Anlage zum BDSG
- Künftig müssen Vorgaben des Art. 32 DSGVO umgesetzt werden
- Abwägung der Maßnahmen nach Schutzbedarfsanalyse
- Anforderungen an Maßnahmen ähnlich den IT-Sicherheitsgesetzen, vgl. § 13 Abs. 7 TMG

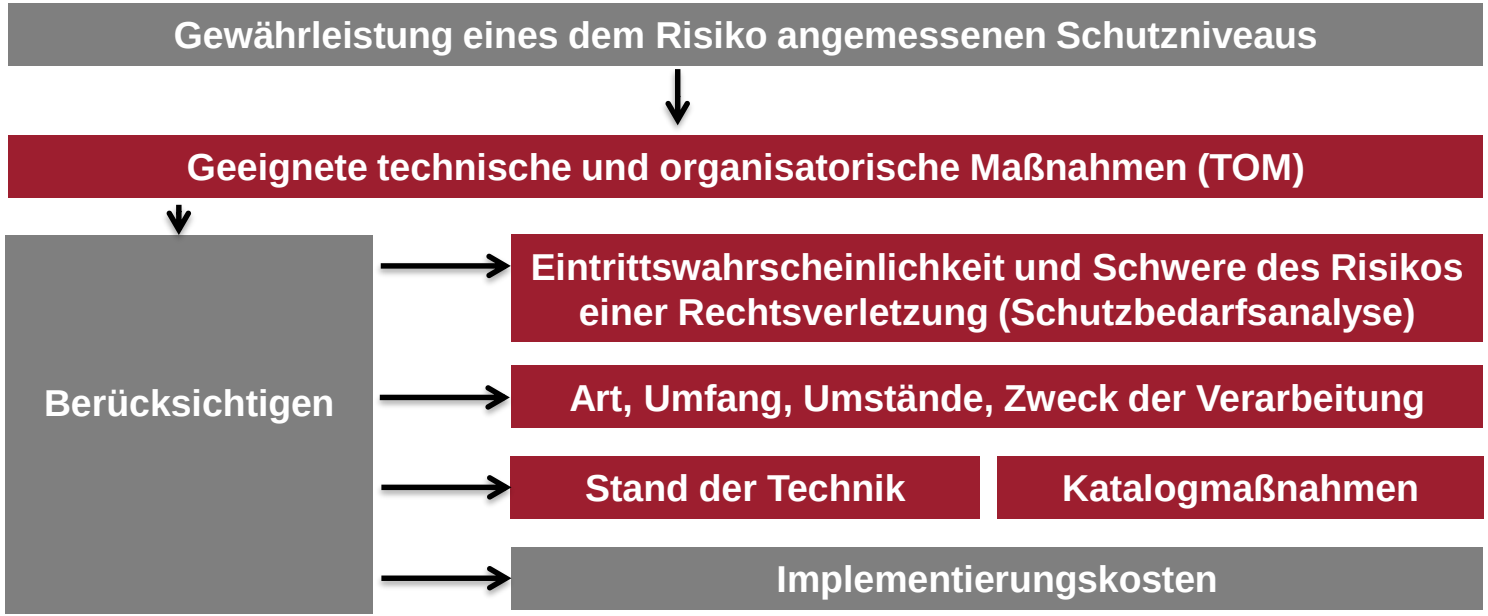
Rechenschaftspflicht gem. Art. 5 DSGVO

(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**“).

HK2 Rechtsanwälte

Art. 32 DSGVO: Sicherheit der Verarbeitung



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 von Wissenschaft und Forschung

Stand der Technik

Anerkannte Regeln der Technik

HK2
Rechtsanwälte

Definition *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.

Ermittlung des Stands der Technik

HK2 Rechtsanwälte

- Innerhalb / außerhalb der Branche
- National / international
- Bewertung

- Beratung
- Arbeitshilfen (Handreichung zum Stand der Technik, TeleTrusT)
- Dokumentation
- Nachweis

DSGVO: Umfangreiche TOM-Dokumentation

- Konsequenz: Pflicht zur umfangreichen Abwägung aller Maßnahmen und Dokumentation des Auswahlprozesses
  - Durchführung einer Schutzbedarfsanalyse zur Bestimmung des erforderlichen Schutzniveaus und der dafür nötigen TOM
  - Abgleich sämtlicher TOM mit dem Stand der Technik: bei Nichteinhaltung Begründungspflicht

- Aus der jetzigen TOM-Liste muss künftig eine umfangreiche TOM-Dokumentation werden

Dokumentation der TOM nach DSGVO

Zugangskontrolle

☒ Zuordnung von Benutzerrechten ☐ Erstellen von Benutzerprofilen

☒ F

☒ A
F

☐ C

☐ S
e

Maßnahmen	Beschreibung	Stand der Technik objektiv-technisch // subjektive Auswahl		Schutzbedarf	Wirksamkeitsprüfung	Wiedervorlage	Verantwortlich/ 4-Augen-Prinzip	Konzern-Mindeststandard

Auftragsverarbeitungs-Vereinbarung, Art. 28 DSGVO

- Auftragsverarbeiter haftet direkt gegenüber Betroffenen
- Keine Beschränkung auf Datentransfer innerhalb EU/ EWR
- Art. 28 Abs. 3 c): **Stand der Technik** muss im Rahmen der TOM berücksichtigt werden

Datenschutz-Folgenabschätzung, Art. 35 DSGVO

- Ähnlich wie § 4d Abs. 5 BDSG, aber größerer Anwendungsbereich
- Beurteilung im Vorfeld der Verarbeitung
  - Voranalyse: wenn „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“
  - Voranalyse identisch mit Abwägung nach Art. 32 DSGVO
- Pflicht zur Konsultation der Aufsichtsbehörde, wenn hohes Risiko festgestellt wird
- Pflicht des Auftragsverarbeiters zur Mitwirkung, Art. 28 Abs. 3 f)

Datenschutz-Folgeabschätzung (DSFA) Art. 35 DSGVO

HK2 Rechtsanwälte

Voranalyse

- Bei **vorrausichtlich hohem Risiko** der Verarbeitung (Prognose), insbesondere,
  - bei Verwendung neuer Technologien
  - nach Art, Umfang, Umstände und Zwecke der Verarbeitung
- Immer bei
  - systematischer u. umfassender Bewertung persönlicher Aspekte natürlicher Personen
  - Verarbeitung bes. Kategorien v. personenbezogenen Daten
  - Überwachung öffentlich zugänglicher Bereiche
  - Ausdrückliche Bestimmung durch Aufsichtsbehörde
- Nie bei
  - Ausdrückliche Bestimmung durch Aufsichtsbehörde

Datenschutz-Folgenabschätzung

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Bewertung von Notwendigkeit und Verhältnismäßigkeit
- Bewertung der Risiken
- Geplante Abhilfemaßnahmen
- …

Hohes Risiko

Normales Risiko

Konsultation mit Aufsichtsbehörde

Empfehlungen

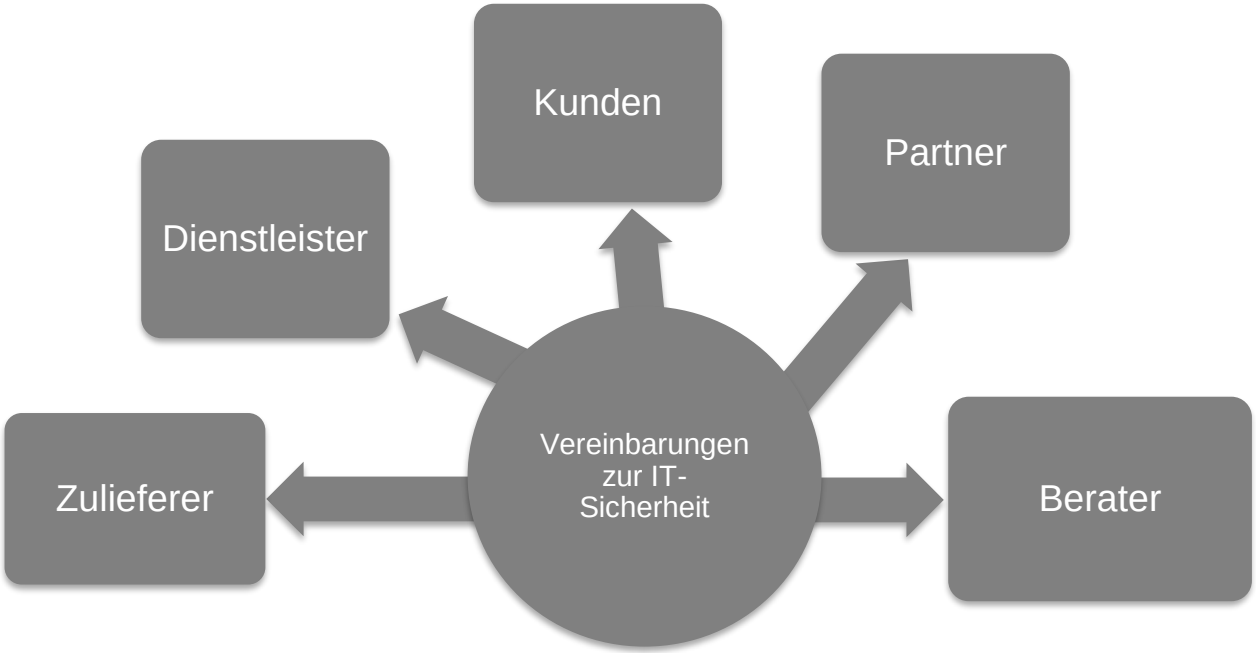
Verarbeitung

Meldepflichten
Art. 33 DSGVO

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und **möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

HK2
Rechtsanwälte

Verträge mit Bezügen zur IT-Sicherheit



Vertragliche Folgen

HK2 Rechtsanwälte

- IT-Sicherheit als Teil der Hauptleistungen
- Schadensersatz wegen Pflichtverletzung
- Vereinbarungen zur IT-Sicherheit mit
  - Kunden
  - Dienstleistern
  - Zulieferern
  - Beratern

HK2
Rechtsanwälte

Sicherungsklauseln

- Konkrete Verpflichtung auf den Stand der Technik
- Kontrolle durch:
  - Information
  - Dokumentation
  - Offenlegung/ Zugang
  - Zugriff
  - Audit
- Anpassung während der Laufzeit
- Absicherung durch Vertragsstrafen, Schadenspauschalen etc.
- Geheimhaltungsklauseln

HK2 Rechtsanwälte

Projektierung der Maßnahmen

- ✓ Differenzanalyse IST - SOLL
- ✓ Datenschutz- und IT-Sicherheitsprozesse prüfen und ggf. anpassen
- ✓ konsolidierte Umsetzung der Maßnahmen planen (ITSiG - DSGVO)

- ✓ Anpassung bestehender Verträge mit IT-Sicherheitsbezug
- ✓ Besonderheit: Vereinbarungen zur Auftrags(daten)verarbeitung an DSGVO anpassen

- ✓ Dokumentieren (neue Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO)
- ✓ regelmäßig revidieren und Umsetzung prüfen

@MerlinBacker