BÜSING MÜFFELMANN & THEYE RECHTSANWÄLTE UND NOTARE

BMT

Datenschutz 2018 - Umgang mit der Datenschutzgrundverordnung (DS-GVO)

Rechtsanwalt Bernd H. Harder, München

Schadenkongress

Leipzig, April 2018

DS-GVO: Die gute Nachricht für Versicherungen

heise online > News > 12/2017 > Immer mehr Cyber-Versicherungen

Immer mehr Cyber-Versicherungen

10.12.2017 16:08 Uhr – Christof Windeck

(Bild: Europol)

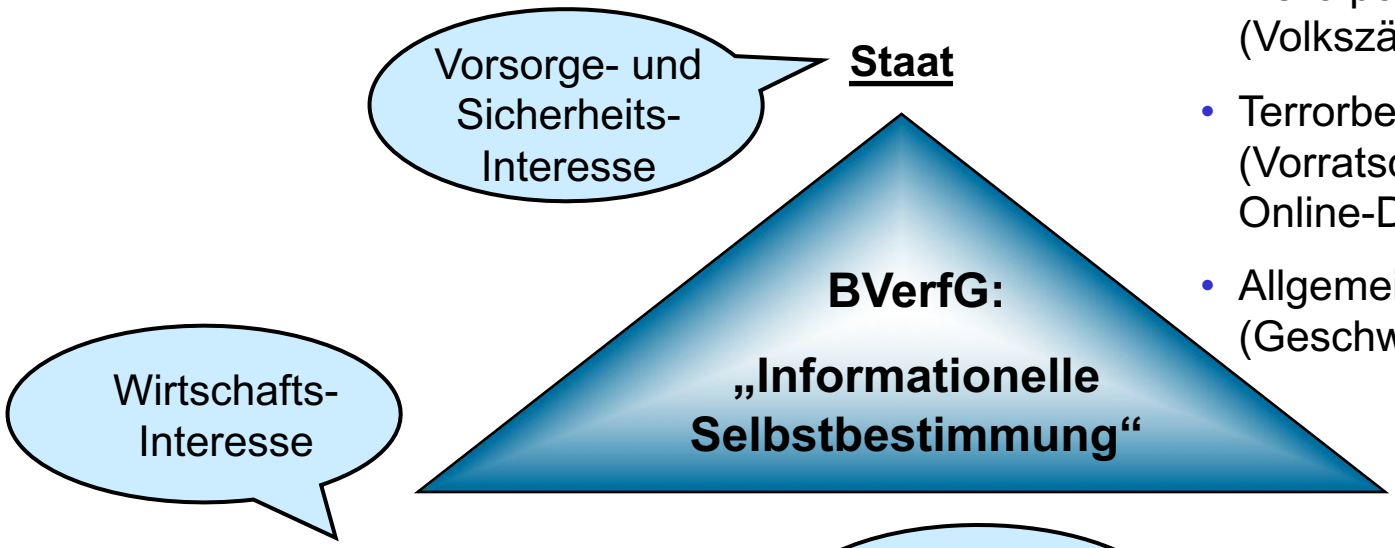
Neue Geschäftspotentiale durch Datensicherheit und Datenschutz!

Mit Cyber-Versicherungen wollen sich Unternehmen häufiger vor den Folgen von Hackerangriffen, Erpressungstrojanern oder auch Datenschutzpannen schützen.

John Chambers, ex-CEO Cisco:
„Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt wurden und diejenigen, die nicht wissen, dass sie gehackt wurden.“

Situation gestern: BDSG bringt kein ROI

Die Ambivalenz des Datenschutzes je nach Perspektive



- Fiskalpolitik / Vorsorge (Volkszählungs-Entsch. 1983)
- Terrorbekämpfung (Vorratsdatenspeich. 2008 / Online-Durchsuchung 2010)
- Allgemeine Kriminalität (Geschwindigkeitsüberw. 2009)

Unternehmen

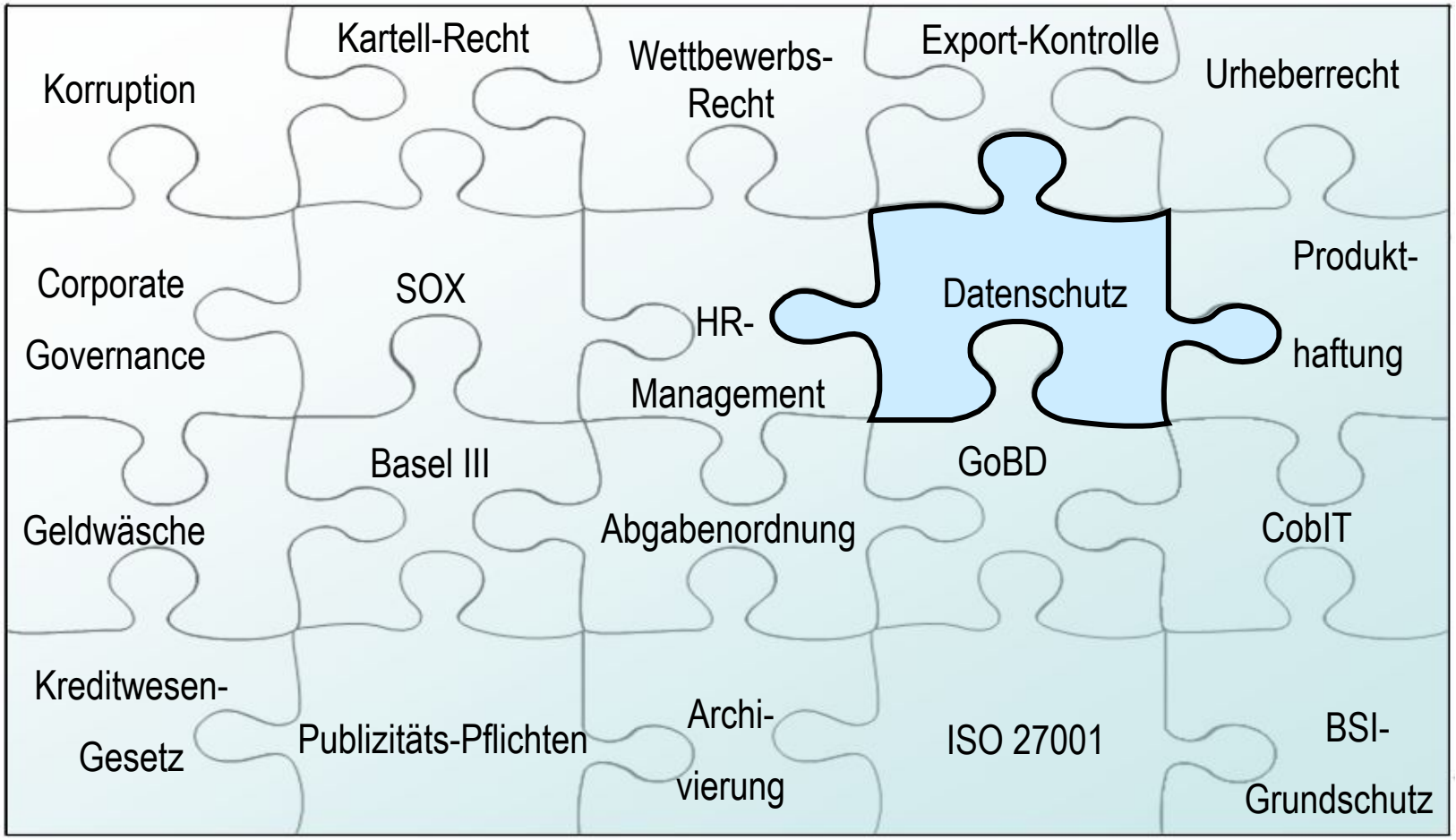
- Outsourcing
- One-to-one Marketing
- MA-Überprüfung

Privatpersonen

- Bürger / Arbeitnehmer
- Kreditkarte
- Facebook-Nutzung

Situation heute: BDSG und Compliance

Das Compliance Puzzle: Datenschutz immer bedeutenderes Puzzle-Teil



Datenschutz gilt nur für „personenbezogene“ Daten

Allgemeine Daten inkl. technischer Daten und Wirtschaftsdaten

- Wetterdaten
- Bilanzen
- Konstruktionsdaten
- Lagerbestandsdaten
- Kostenaufstellungen
- Statistiken

⋮

- Standortdaten ?

Thema: Datensicherheit

Personenbezogene Daten (BDSG)
- Name
- Anschrift
- Geburtsdatum
- Berufsbezeichnung
- Telefon – Nummer
- …

Persönliche Daten
- Telefongespräche
- E-Mail
- …

Besondere Arten personenbezogener Daten
- Gesundheit
- Rasse
- Religion
- …

- Berufsgeheimnisse (Ärzte, Rechtsanwälte)
- Angaben hinsichtlich strafbarer Handlungen
- Bank- oder Kreditkartenkonten

einfacher Schutz **verstärkter Schutz** **besonderer Schutz**

BDSG: Verbotsprinzip mit Erlaubnisvorbehalt

Verarbeitung personenbezogener Daten grundsätzlich unzulässig*…

Zulässigkeit

- **Einwilligung des Betroffenen** (**„Schriftform,** künftig nicht mehr erforderlich)
- **Gesetzliche Erlaubnis**
  - zur Erfüllung eines Vertrages
  - zur Erfüllung einer rechtlichen Verpflichtung
  - zum Schutz von lebenswichtigen Interessen
  - zur Wahrnehmung einer Aufgabe im öffentlichen Interesse
  - zur Wahrnehmung berechtigter und überwiegender Interessen des „Verantwortlichen“

*Art. 6 DS-GVO (bisher § 4 BDSG)

…richtiger Ansatz in der Informationsgesellschaft, um Missbrauch zu vermeiden?

Kartellrecht hier eher angebracht

Zielgruppe und Leitbilder für die DS-GVO…

… aber alle Unternehmen unterliegen den rigiden Bestimmungen!

Situation morgen: 25. Mai 2018

BMT

➢ Wesentliche Neuerungen in der DS-GVO gegenüber BDSG:

- ✓ – **Datenschutz durch Technikgestaltung und durch datenschutz-freundliche Voreinstellung (Privacy by Design) – Art. 25**
- (✓) – **Datenschutz-Folgenabschätzung – Art. 35**
- (✓) – **Verantwortlichkeit / Zuständigkeit (Art. 24, 26, 28)**
- (✓) – **Recht auf Löschung („Recht auf Vergessenwerden“) – Art. 17**
- ? – **Recht auf Datenübertragbarkeit – Art. 20**
- ((✓)) – **Weitreichende Informationspflichten – Art. 13, 14, 15, 33, 34**
- ! – **Drastische Sanktionen – Art. 83**

Hoher Anpassungs-aufwand in der IT

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU

„Verantwortlicher“ ist letztlich die Geschäftsleitung

Art. 4 DS-GVO (Begriffsbestimmungen)

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

⋮

7. “Verantwortlicher” die **natürliche** oder **juristische Person,** Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der **Verarbeitung** von personenbezogenen Daten **entscheidet;**

⋮

… aber im Zweifel kann die Geschäftsleitung nicht selbst unmittelbar beurteilen, ob eine personenbezogene Datenverarbeitung vorliegt.

➡ Mitarbeiter (Fach- / IT-Abteilung, Datenschutzbeauftragter) sind in den Prüfungsprozess mit einzubeziehen.

Der Bußgeld-Rahmen*

Drastische Erweiterung der Sanktionsmöglichkeiten

- Bis **10 Mio.** EUR oder bei Konzernen bis **2 %** des weltweiten Jahres-Umsatzes bei u.a.
  - Verstoß gegen die elterliche Einwilligung bei Kindern
  - Verstoß gegen das Privacy by Design-Prinzip
  - Verstoß gegen die Dokumentations-Pflichten

- Bis **20 Mio.** EUR oder bei Konzernen bis **4 %** des weltweiten Jahres-Umsatzes bei u.a.
  - Verstoß gegen Rechte der betroffenen Personen
  - Verstoß gegen unberechtigten Daten-Transfer in Drittstaaten
  - Verstoß gegen behördliche Auflagen

***Art. 83 DS-GVO (BDSG: bis 300.000,00 EUR)**

Zusätzlich: Strafvorschriften

§ 42 BDSG (neu)

(1) …

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

(1) ohne hierzu berechtigt zu sein, **verarbeitet** oder

(2) durch unrichtige Angaben erschleicht

und **hierbei gegen Entgelt** oder in der Absicht **handelt,** sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) …

⋮

Trifft den Handelnden, nicht das Unternehmen!

Wichtige Organe und DS-Aufsichtsbehörden

sog. Art. 29-Gruppe

- seit 1995
- berät die EU-Kommission
- gibt Empfehlungen und Stellungnahmen
- besteht aus je 1 Vertreter der jeweiligen nationalen DS-Behörden
- bis 24.05.2018

Europäischer Datenschutzausschuss

- ab 25.05.2018
- Aufgaben ähnlich Art. 29-Gruppe
- besteht aus dem Europäischen DS-Beauftragten und den Leitern der jeweiligen nationalen DS-Behörden (Dtl.: Bundes-Datenschutzbeauftragte und 1 Vertreter der Landesaufsichtsämter)

Deutsche Datenschutzaufsicht

- besteht aus Bundes-DS-Beauftragter (BDSG) und 17 Landes-DS-Aufsichtsbehörden (Landesdatenschutz-Gesetze)
- Abstimmung bisher im Düsseldorfer Kreis, künftig in sog. Kohärenzverfahren

DS-GVO Projekt wird in 4 Phasen durchgeführt

BMT

1. Analyse Status/Gap → **2. Maßnahmen Tech./Org.** → **3. Priorisierung/ Verantwortlichkeit** → **4. Umsetzung/ Review**

- Datenschutz-Policy
- Verarbeitungs-Verzeichnis
- Privacy-by-Design Prozess
  - Risikoanalyse
  - DS-Folgenabschätzung
- ADV und Vereinbarungen
  - ADV-Verträge
  - Verpflichtungen auf Datengeheimnis
  - Betriebsvereinbarungen
- Datentransfer in Drittländer
- Ablaufregelungen für
  - Informationspflichten
  - Auskunftserteilung, Berichtigung, Widerspruch
  - Löschung
  - Datenübertragbarkeit
  - Pflichten bei Datenpannen
- Mitarbeiter-Schulung

- Aktionsplan zur Aktualisierung der gesetzlichen Vorgaben
  - organisatorische Anweisungen und Verträge
  - technische Maßnahmen
- Definition von Bemessungskriterien
- Schulungskonzept-Anpassung
- Absprache mit Betriebsrat

- Priorisierung der erforderlichen Maßnahmen nach
  - Risiko
  - Aufwand
  - Kapazität
- Eindeutige Zuordnung der Verantwortlichkeit je Maßnahme

- Parallele/sequenzielle Einführung der erforderlichen Maßnahmen unter Mitwirkung aller (involvierten) Unternehmens-Bereiche
- Bestimmung von Meilensteinen für Kontrollmaßnahmen zur Qualitätssicherung
- Review der Gap-Analyse

vielfach unterschätzter Aufwand!

DSGV-Vorbereitung: Fertigstellungsgrad

Firma:	
	Muster Gmbh & Co KG
Datum:	
	3.2.2018
Fertigstellungsgrad:	
	0%

21	Ein Verzeichnis aller Verarbeitungstätigkeiten gemäß Art. 30 und 32 DS-GVO ist erstellt und auf Aktualität und Vollständigkeit geprüft.	☐ Erstellt ☐ Geprüft
22	Ein Prozess zur Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten ist dokumentiert und implementiert.	☐ Dokument ☐ Umgesetzt
23	Ein Prozess zur grundrechtskonformen Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO ist dokumentiert und implementiert.	☐ Dokument ☐ Umgesetzt

GDRP Readliness Assessment

- über 80 Fragen
- Antworten fließen gewichtet in %-Satz des Fertigstellungs-grads ein

Fazit

BMT

DS-GVO: ein Gesetz für die Vergangenheit…

- **Kein zeitgemäßes Regelungswerk für die Informationsgesellschaft**
  - **aufgeblähtes Verarbeitungsverbot statt klare Missbrauchs-Bekämpfung**
  - **um 5 Marktteilnehmer zu treffen, über 3 Millionen belastet**
  - **keine zukunftsorientierte Lösungsansätze (IoT, KI)**
- **Zahlreiche unbestimmte Rechtsbegriffe und praxisferne Vorgaben (insbesondere in Erwägungsgründen) werden zu langwierigen Auslegungs-Auseinandersetzungen führen**
- **Hohe Umstellungskosten in der IT und hoher organisatorischer Anpassungsaufwand**
- **Nächstes Desaster droht 2019 (aus Zeitgründen nicht angesprochen): E-Privacy Verordnung-ähnlicher Regelungsinhalt, anderes Vokabular!**

… aber jeder muss sich damit auseinandersetzen!

Vielen Dank

für Ihre Aufmerksamkeit!

Rechtsanwalt Bernd H. Harder
Maximilianstraße 38, 80539 München
Telefon: 089/287007-0
Telefax: 089/287007-29
Homepage: www.bmt.eu