DatenSchutzGrundVerOrdnung
eine Übersicht

DI Martin Schober

MSc – martinschober.com

IT-Cloud & Security Consultant

Certified Data & IT Security Expert

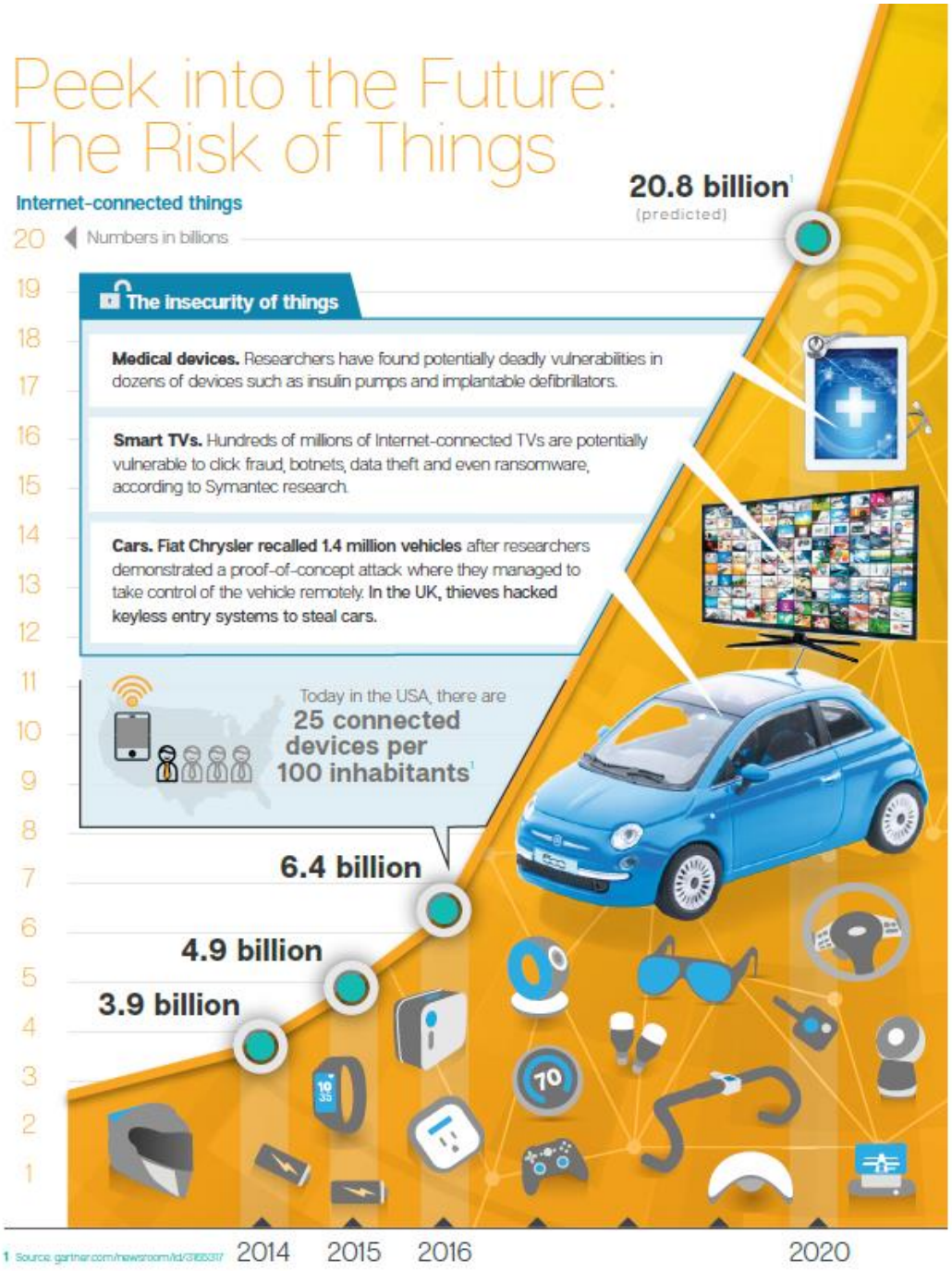
CERTIFIED
DATA & IT SECURITY
EXPERT

Martin Schober – zur Person

- Gründer: MSc-martinschober.com (2003)
  - Mitarbeit: Siemens UMTS-Standard
  - Baxter BioScience: TQM-Management
- IT- & Cybersecurity
- Cloud-Consultant für Outsourcing, SLAs
- Sprecher der IT-Security Experts Group Salzburg
- ISO & BSI Auditor (IT-Sicherheit)
- Datenschutz-Beauftragter für Unternehmen
- **IT-ThinkTank**

IoT: Internet of Things

- Mirai-Botnet
- Bricker Botnet



Heute:
25 IoT auf 100 US-Einwohner

Was?
Autos, Flugzeuge, Schlösser, Insulinpumpen, Thermostat, Herzschrittmacher, Licht, Fenster, Kaffeemaschinen, …

2020:
20.800.000.000 Geräte für
8.000.000.000 Menschen

Daten
sind die Rohstoffe des 21. Jhds

General Data Protection Regulation

Ist seit 25.05.2016 in Kraft!

Umsetzung: 25. Mai 2018


UND?
„DIE ZAHLREICHEN INFORMATIONEN ÜBER SIE UND IHRE BILDER IM NETZ HABEN UNS HEITERE KURZWEIL BEREITET. WIR WÜNSCHEN IHNEN VIEL ERFOLG AUF IHREM WEITEREN LEBENSWEG."
BEWER-BUNG ABSAGE

DSGVO – **D**aten**S**chutz**G**rund**V**er**O**rdnung

- *260 Seiten*
- *173 ErwGründe*
- *69 Öffnungsklauseln*
- *11 Kapitel*
- *99 Artikel*
- *Ende der Umsetzungsfrist:*

  25. Mai 2018

Dann ist DSG 2000 nicht mehr anwendbar & *DSRL 96/46/EG* aufgehoben!

Achtung: *Umstellungen in der IT notwendig!*

Verzeichnis der Kapitel

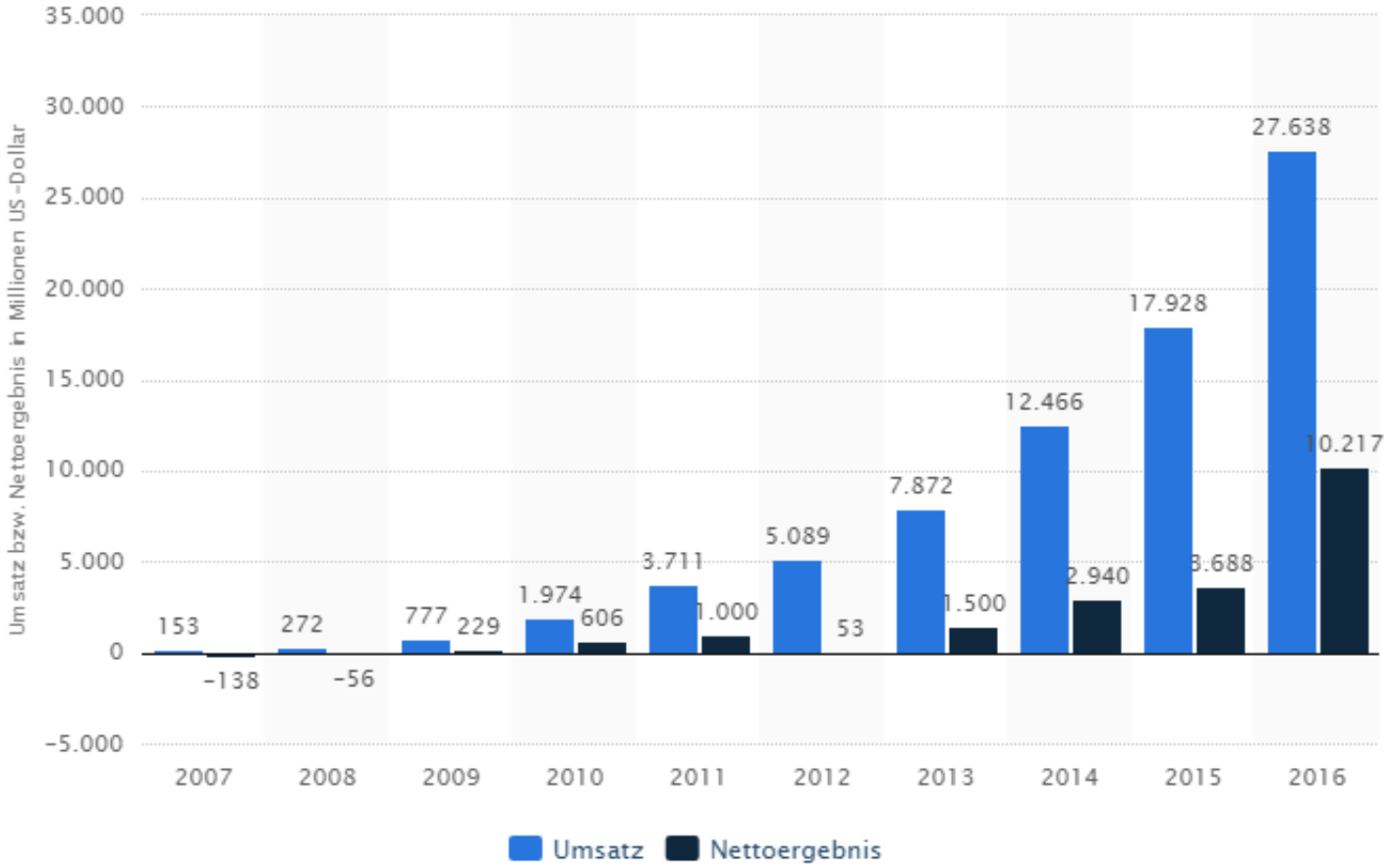
Warum brauchen wir die DSGVO?

Problemkreise

- Globalisierung
- Internet allgemein
- Mobiles Internet
- Internet der Dinge
- Industrie 4.0
- Cloud-Computing
- Soziale Netzwerke
- GPS

- RFID
- Automatisierte Verfahren zur Datengewinnung
- Unzureichende Harmonisierung der europäischen Datenschutz-Gesetze

Umsatz und EBIT Facebook



https://de.statista.com/statistik/daten/studie/217061/umfrage/umsatz-gewinn-von-facebook-weltweit/

Sinn der DatenschutzVO

- Mehr Kontrolle für EU-Bürger
  - Recht auf Vergessen, Hoheit über Löschungen
- Einfachere Verwaltung
  - One Stop Shop Prinzip (Sitz!)

Zur Erinnerung:
Daten sind die Rohstoffe des 21. Jhds

- Betrifft Unternehmen mit Niederlassung in EU
- Was tun bei einem Leck? Defin. Vorgehen

Für wen gilt diese VO?

1. Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen!

2. Diese Verordnung findet **keine Anwendung** auf die Verarbeitung personenbezogener Daten,

a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,

b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, […]

Wichtigsten Änderungen

- Einwilligung & Auskunftsrecht
- Umfassende Informationspflichten
- Entfall der DVR (Meldepflicht)
- Recht auf Vergessenwerden
- Dokumentationspflichten (ErwG13: Erleichterungen für KMUs)
- Datenschutz-Folgenabschätzung
- Hohe Strafen: 2% (10 Mio) und 4% (20 Mio) vom Jahresumsatz
- Datenschutz für jur. Personen entfällt
- Markortprinzip
- Bereichsspezifische Datenverarbeitung
- Datenschutzbeauftragter
- Datensicherheit
- Datenportabilität
- Data Protection by Design/Default

Was sind KMUs i.S. DSGVO?

ErwG 13: Erleichterungen für KMUs → Verfahrensverzeichnis

	Beschäftigte	Umsatz in € Mio.	Bilanzsumme in € Mio.
Kleinstunternehmen	9	2	2
Kleinunternehmen	49	10	10
Mittlere Unternehmen	249	50	43

Definition: personenbezogene Daten

alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche Person beziehen**;

als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Definition: Verarbeitung

jeden **mit** oder **ohne Hilfe automatisierter Verfahren** ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit **personenbezogenen Daten** wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Verantwortliche

- Geschäftsleitungsorgane (Vorstände, Geschäftsführer)
  - Letztverantwortlichkeit für die Einhaltung des DS
  - Verantwortlichkeit für die Auswahl und Ausstattung des DSB
- Ansprechpartner aus den Abteilungen/Bereichen
  - Informationspflicht in Bezug auf neue oder geänderte Datenanwendungen
  - Informationspflicht bei DS-Vorfällen
- Informationseigentümer
  - Datenqualität
  - Einstufung Schutzbedarf
- Informationstreuhänder
  - App-Verantwortung IT
  - Systemadmin
- Informationsbenutzer / MA
  - Einhaltung DS Regeln
  - Meldung DS-Vorfälle

Datenschutzbeauftragter - Pflichten

- DSB ist weisungsfrei; kein Interessenskonflikt;
- Unterrichtung und Beratung des Verantwortlichen und der MA
- Überwachung der Einhaltung dieser Verordnung
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für Fragen

Datenschutzbeauftragter - Rechte

- Aktive Unterstützung des Datenschutzbeauftragten durch Führungskräfte
- Ausreichend Zeit zur Wahrnehmung der Pflichten des DSB
- Ausreichende Unterstützung in Bezug auf Finanzmittel, Infrastruktur - auch MA
- auch Datenschutz-Team ist möglich
- Name muss keiner genannt werden! @

Was tun als Unternehmer?

- Zeit bis 25. Mai 2018:
  - Man muß **JETZT** anfangen
  - Projekt-Fahrplan erstellen - Timeline
  - Umsetzen und Dokumentieren
  - Risikomanagement - Kategorien
  - Sicherheitskonzepte erstellen
  - Archivierung & Löschung definieren
  - GAP-Analyse: **Soll – Ist** Vergleich <- damit beginnen!

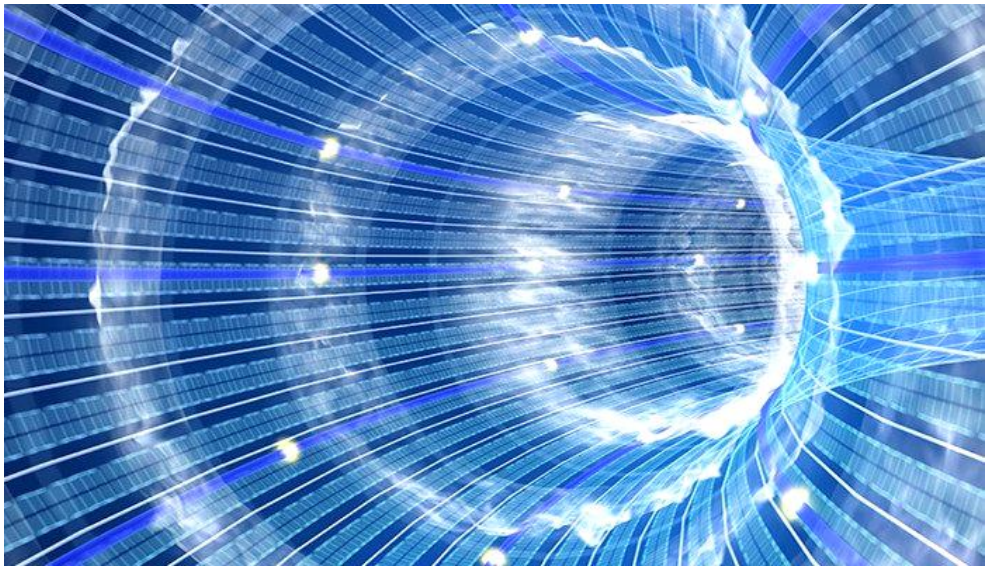
... wir helfen gerne!

Fragen die Sie sich stellen sollten:

- Welche Formen von Missbrauch wären möglich, wenn vertrauliche Informationen Ihres Unternehmens oder Ihrer Organisation in die Hände Dritter gelangten?
- Welche Konsequenzen hätte es für Sie, wenn wichtige Informationen verändert würden oder verloren gingen? nicht nur böse Absicht sondern auch technisches Versagen
- Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfielen und einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?

Gefahren

- **Datenverlust**
- **Datendiebstahl**
- **Virenbefall**
- **Hacker**
- **Administratorausfall**
- **Systemausfall**
- **Rechtlichen Konsequenzen**



Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess

DSMS - Dokumentation

1. DS-Politik
2. Aufbau DS-Richtlinie
3. Auskunftsverfahren
4. DS-Konzepte & Berichte
5. DS-VerfahrensVZ
6. Sicherheitsmaßnahmen & Protokollierung
7. DS-Handbuch & Awareness-Schulungen
8. Löschkonzept

Ende

- Fragen
- Anmerkungen
- Diskussion

DI Martin Schober

IT- & Cybersecurity

http://www.martinschober.com

office@martinschober.com

+43.660.1517017

DatenSchutzGrundVerOrdnung
eine Übersicht

DI Martin Schober

MSc – martinschober.com

IT-Cloud & Security Consultant

Certified Data & IT Security Expert

CERTIFIED
DATA & IT SECURITY
EXPERT