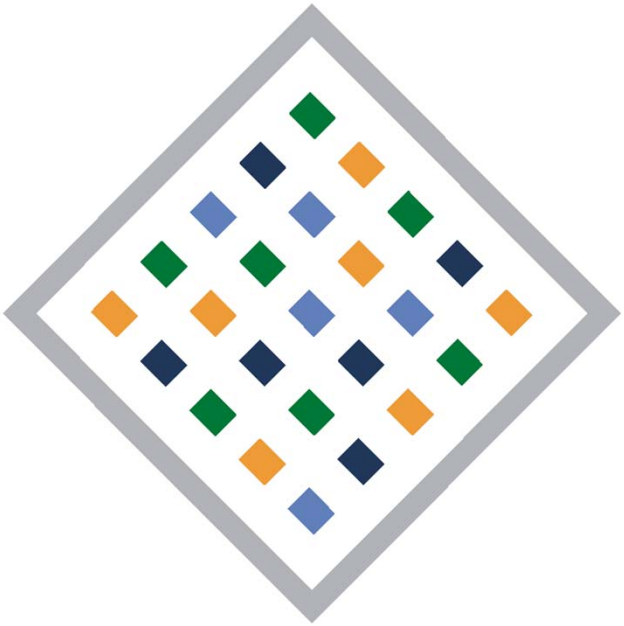
5. Stralsunder IT-Sicherheitskonferenz



Smartphone, Internet of Things und Co. - Datenschutz im Zeitalter einer mobilen Welt

Thomas Brückmann

Mitarbeiter

beim Landesbeauftragten für Datenschutz und Informationsfreiheit

Mecklenburg-Vorpommern

Agenda

1. Datenschutz?
   - Wer wir sind und was wir machen
2. Rechtsgrundlagen
   - Die aktuelle Rechtsgrundlage
   - Die aktuelle Lage
   - Die zukünftige Rechtsgrundlage
3. Internet der Dinge
   - „Beleuchtung der Dinge“ / Definition
   - Beispiele und Gefahren
4. (Kurz-)Fazit / ToDo‘s

Rechtsstellung der Landesdatenschutzbeauftragten

- Wahl durch das Parlament (6 Jahre Amtszeit)
- Organisatorische Anbindung bei Landtagspräsidentin
- Unabhängig und weisungsfrei (keine Fach- oder Rechtsaufsicht seit 2011; Dienstaufsicht der Landtagspräsidentin nur soweit Unabhängigkeit nicht tangiert)
- Oberste Dienstbehörde i. S. v. § 96 StPO u. Oberste Aufsichtsbehörde i. S. v. § 99 VwGO

Aufgaben und Befugnisse des Landesbeauftragten

- Bearbeitung von Petitionen
- Beratung bei der Erarbeitung von Gesetzentwürfen
- Kontrolle der Einhaltung gesetzlicher Vorschriften
- Beratung von Behörden und Unternehmen
- Erarbeitung von Gutachten
- Information der Öffentlichkeit
- Zusammenarbeit mit anderen Datenschutzinstitutionen
- Beobachtung der Entwicklung der IuK-Technik
- ...

Das Amt des LfDI M-V

Der Landesbeauftragte für Datenschutz und Informationsfreiheit

LD 1 Recht / IFG

- Polizei
- Justiz
- Verfassungs-schutz
- Ausländerrecht
- Religion
- Einwohnerwesen
- Kommunales
- Geodaten
- Umweltschutz
- Informations-freiheit

LD 2 Gesundheit / Soziales

- Grundsatzfragen
- Europa
- Finanzen / Steuern
- Statistik
- Sozialwesen
- Gesundheits-wesen
- Personal
- Beschäftigten-DS
- Bildung
- Wissenschaft
- Landwirtschaft

LD3 Technik / Verwaltung

- IT-Planungsrat
- AK Technik
- E-Government
- TK und Medien
- IT-Sicherheit
- IT-Management
- Biometrie
- Soziale Netze
- Organisation
- IT Dienststelle
- Allgemeine Verwaltung

LD 4 Wirtschaft

- Banken
- Kreditwirtschaft
- Versicherungen
- Auskunfteien
- Wohnungswirtschaft
- Handel
- Versandhandel
- Handwerk
- Industrie
- Verkehr
- Videoüber-wachung

Die (aktuelle) Rechtslage

Rechtsgrundlagen

Grundgesetz

Artikel 1
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung allerstaatlichen Gewalt.

Artikel 2
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

EU-Grundrechte-Charta

Artikel 1 - Würde des Menschen
Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.
Artikel 8 - Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf *Schutz der sie betreffenden personenbezogenen Daten*.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit *Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage* verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer *unabhängigen Stelle überwacht*.

Das Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983:

Das Grundrecht auf informationelle Selbstbestimmung leitet sich ab aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG.

Das Grundrecht gewährleistet die **Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.**

Das Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß.“

Das bedeutet: Wir leben nicht mehr in einem modernen Rechtsstaat, wenn wir die Kontrolle über unsere Daten verlieren.

BVerfG Volkszählungsurteil 1983 – noch zeitgemäß ?

Rechtsgrundlagen

	öffentliche Verwaltung	„nicht-öffentlicher“ Bereich § 2(4)	Privatpersonen
Europa	Verordnung(EG) Nr. 45/2001	RL 95/46/EG	
Bund	1. spez. Bundesgesetze 2. §§ 1-26 BDSG	1. spez. Bundesgesetze 2. §§ 1-11, 27ff. BDSG	
Land Kreis/ Gemeinde	1. spez. Bundes- 2. und spez. Landesgesetze 3. DSG M-V	1. spez. Bundesgesetze, sonst 2. BDSG	§ 1 (2) Nr.3 BDSG

Rechtsgrundlagen

Grundtenor: Verbot mit Erlaubnisvorbehalt!

Lösung: informierte Einwilligung § 4a(1) BDSG, § 7 DSG M-V

- Wirksamkeit setzt **Einsichtsfähigkeit** voraus, d.h. Fähigkeit, Tragweite und Folgen der Erklärung abzuschätzen
- Hinweis auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung

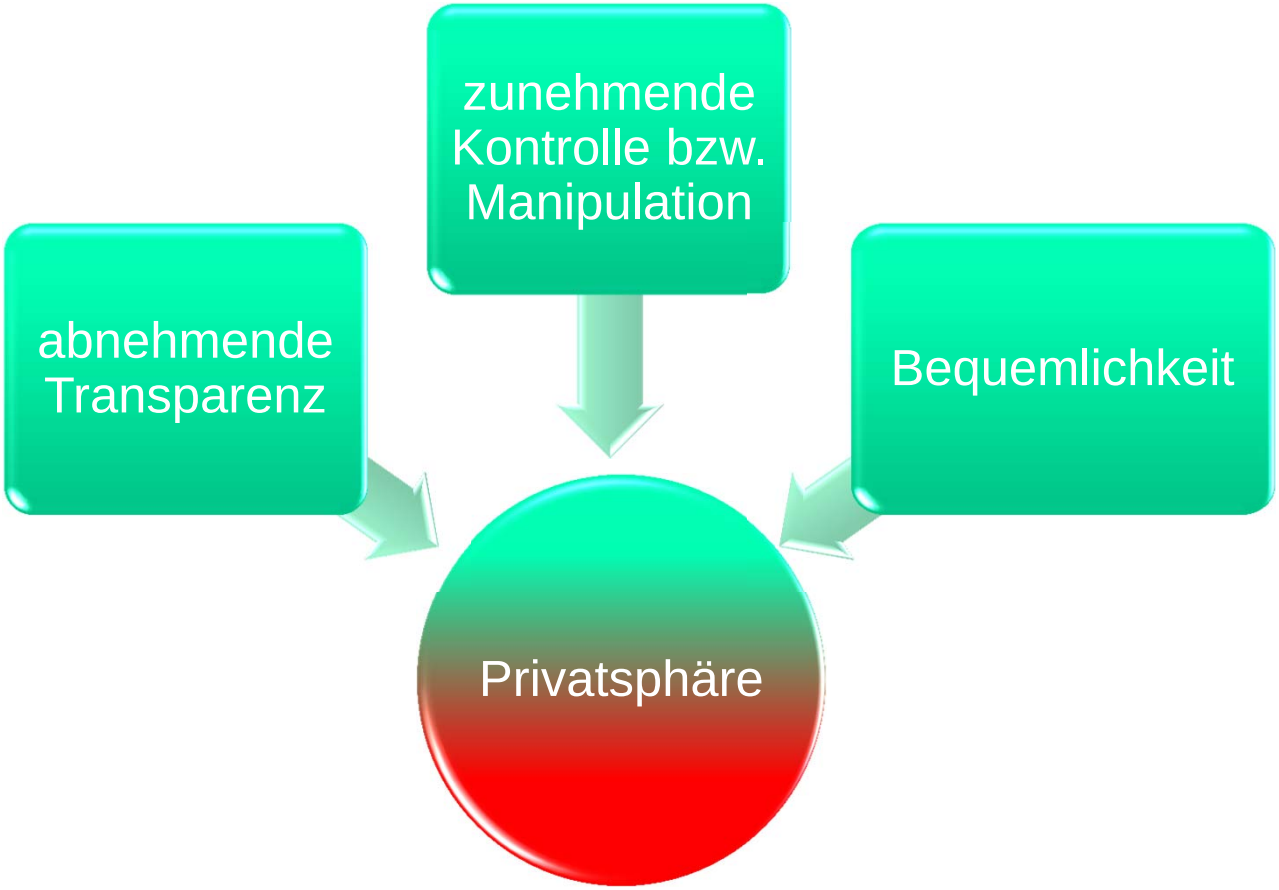
- Formen der Einwilligung:
  1. Ausdrücklich, schriftlich (Regelfall)
  2. Konkludent (durch schlüssiges Verhalten)
  3. Mutmaßlich (nur als (begründete) **Ausnahme** möglich)

Die aktuelle Lage

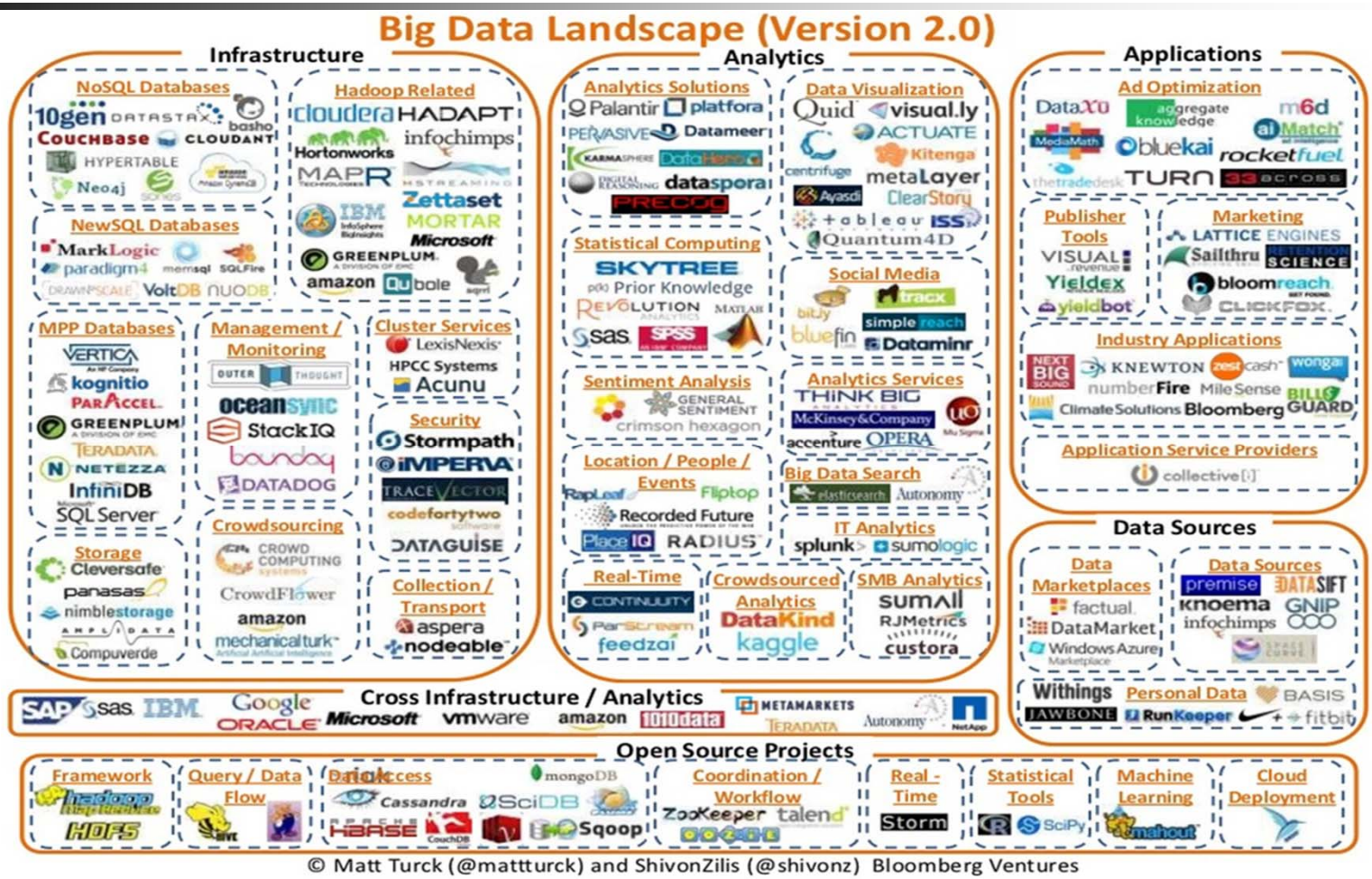
Digitale Grundrechte im Schützengraben

- Data-Warehouse, Datamining, Adresshandel, Scoring
- RFID-Chips und Bionik – die „Intelligenz“ der Technik: ubique computing
- **Internet of Things**
- **Cloud Computing, Big Data**
- **Smart Metering, Smart Home, Smart Living, Smart Health,...**
- Internetüberwachung (E-Mail, Cookies, Ortung, GPS etc.)
- Quantified Self
- Bewegungsprofile (Maut, Handyortung, Gesichtserkennung, Kennzeichenregistrierung, Funkzellenüberwachung, GPS, PRISM …)
- biometrische Datenbanken (Finger, Iris, Gesicht,)
- digitaler Fingerprint von Computern und Smartphones
- Vorratsdatenspeicherung (nicht nur bei Providern)
- INDECT-Überwachungs- und Sicherheitssysteme
- selbst entscheidende Algorithmen
- …..

Risiken für das Grundrecht „Privatsphäre“

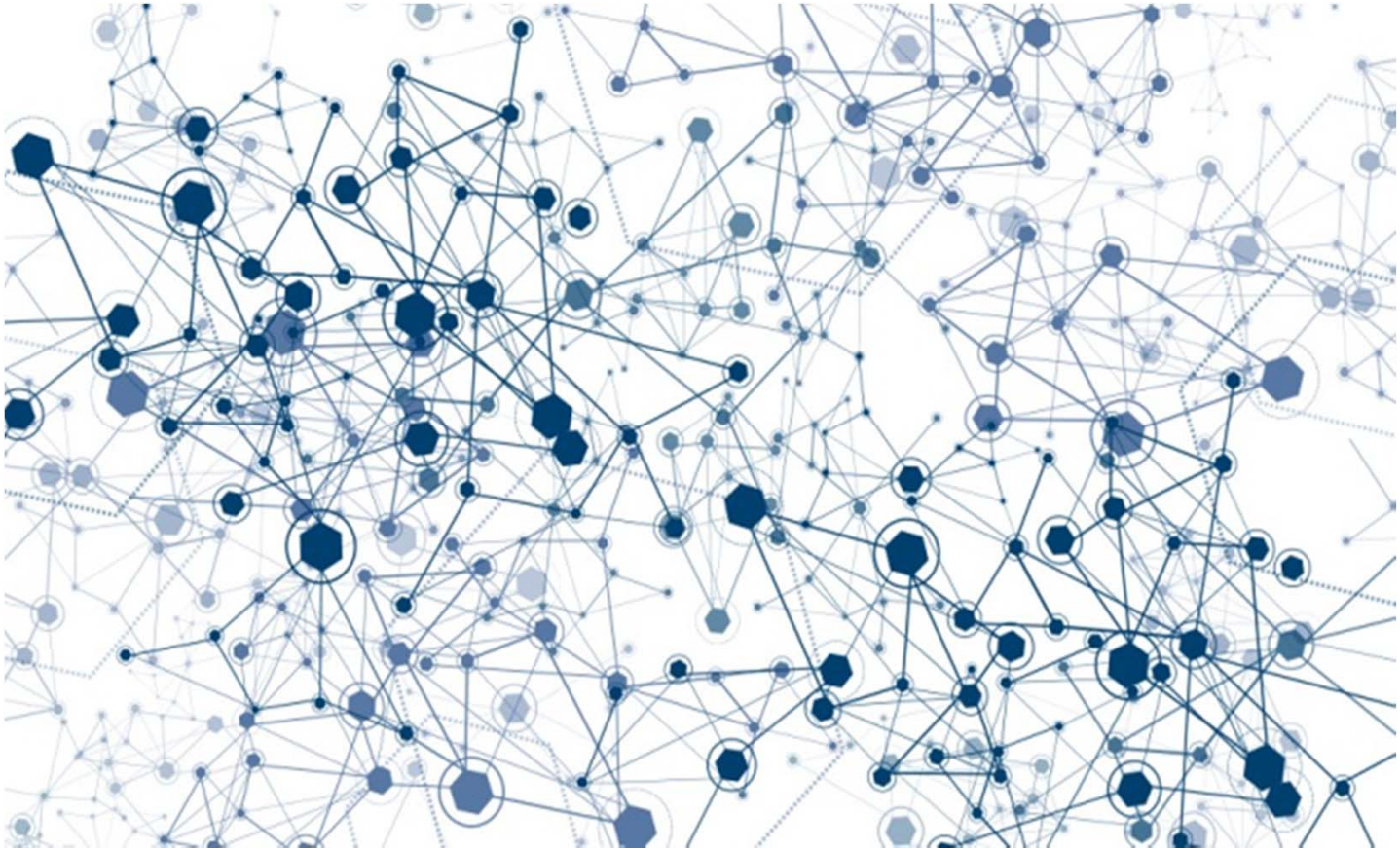


… die Zukunft ??



© Matt Turck (@mattturck) and ShivonZilis (@shivonz) Bloomberg Ventures

Die Konsequenz



Zwei Jahre digitale Agenda: "Cloud hört sich an wie Stehlen"

heise online 06.09.2016 19:10 Uhr – Stefan Krempl vorlesen

Thomas de Maizière, Sigmar Gabriel und Alexander Dobrindt bei eco. (Bild: heise online, Stefan Krempl)

Die drei federführenden Minister der digitalen Agenda sind sich einig, dass das Prinzip der Datensparsamkeit weg muss. Das Thema Datensicherheit sei eines der großen Digitalisierungshemmnisse für kleine und mittlere Unternehmen.

Die Lösung ???

Die Europäische Datenschutz-Grundverordnung
(25. Mai 2018)

Europäische Datenschutz-Grundverordnung

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung – DS-GVO)

Parlamentum Europaeum

Europäische Kommission

Ziele der DS-GVO

- **Kontrolle** über Daten im Sinne der digitalen Grundrechte
- **globale Standards** für Datenschutz
- **Optimierung des modernen digitalen Binnenmarktes**
  - **Harmonisierung** (EUR 2,3 Milliarden Einsparungen durch Vereinheitlichung unterschiedlicher Datenschutzregeln)
  - **Vereinfachung** (EUR 130 Millionen Einsparung durch Abschaffung von Meldepflichten)
  - **kein „Forum-Shopping“** (Datenverarbeitung in Mitgliedsstaat mit weniger strengem Datenschutzrecht)
  - **„One-Stop-Shop“** (eine zuständige Aufsichtsbehörde für Unternehmen in der Europäischen Union)
  - **Kooperationverpflichtung** der Datenschutzaufsichtsbehörden
  - **Konsistenz** der Anwendung des Datenschutzrechts

Wirkungen der DS-GVO

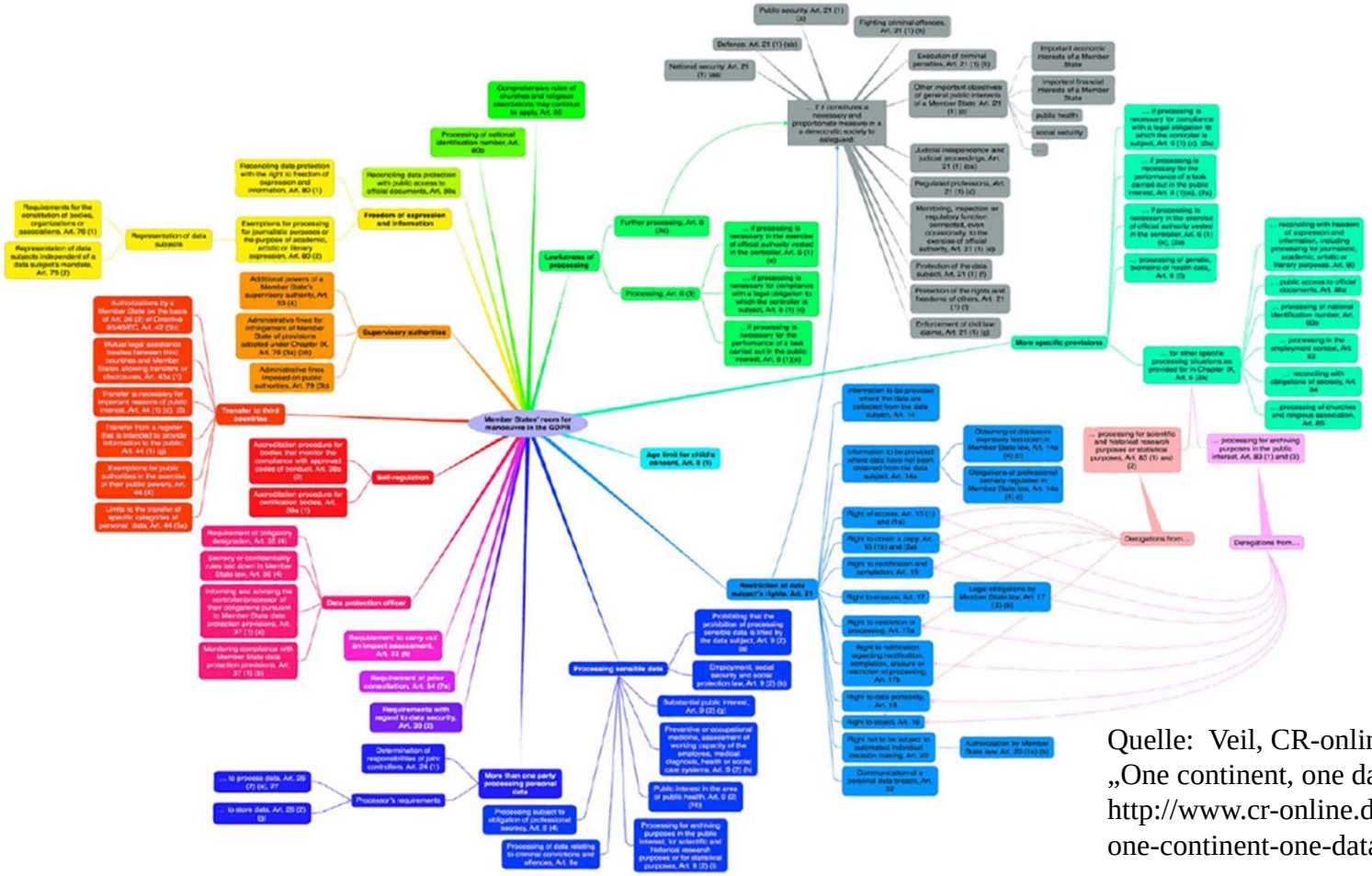
Art. 99: *„ … Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“*

- die DS-GVO ist eine Regelung mit unmittelbarer innerstaatlicher Geltung -> sog. **„Durchgriffswirkung“**
- grundsätzliche Vollharmonisierung (tendenziell weniger im öffentlichen Bereich)
- ersetzt nationales Datenschutzrecht, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen und zur Überflüssigkeit inhaltlich gleicher Regelungen
- Öffnungsklauseln für nationalen Gesetzgeber in bestimmten Bereichen – daher „Richtlinien-Charakter“ im öffentlichen Bereich

~~BDSG~~
~~LDSG~~

➡ **Zweijährige** Anpassungsphase für Rechtsbereinigung und Folgeänderungen

Öffnungsklauseln - Überblick



Quelle: Veil, CR-online 1. Februar 2016
„One continent, one data protection law?“
http://www.cr-online.de/blog/2016/ 02/01/
one-continent-one-data-protection-law/

Begriffsbestimmungen

neue Begriffe in Art. 4 DS-GVO:

- Verletzung des Schutzes personenbezogener Daten
- **genetische, biometrische, Gesundheitsdaten**
- Unternehmen, Unternehmensgruppe, Hauptniederlassung
- Vertreter
- verbindliche unternehmensinterne Datenschutzvorschriften
- **Aufsichtsbehörde, betroffene Aufsichtsbehörde**
- **grenzüberschreitende Verarbeitung personenbezogener Daten**
- maßgeblicher und begründeter Einspruch
- Dienst der Informationsgesellschaft
- internationale Organisation

neue Terminologien und Instrumente

- **Kinder**
- gemeinsam Verantwortliche
- **Datenschutz-Folgenabschätzung**
- **Vergessenwerden**
- Einschränkung der Verarbeitung
- **Datenübertragbarkeit**
- **Profiling**
- vorherige Konsultation
- **Zertifizierung**
- Kohärenzverfahren
- …

Grundsätze für die Datenverarbeitung – Art. 5

„(1) Personenbezogene Daten müssen
a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, ***Transparenz***“);
b) für ***festgelegte, eindeutige und legitime Zwecke*** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (***„Zweckbindung“***);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (***„Datenminimierung“***);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, ***unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)***;“

Grundsätze für die Datenverarbeitung – Art. 5

„(e) ***in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist***; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch 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***“).“

Was tun im Datenschutz-Dschungel?

Quelle: Lizzard / Pixelio.de

Überblick Standard-Datenschutzmodell (SDM)

heise online > News > 2015 > KW 40 > Datenschützer verabschieden neues Prüfmodell

« Vorige | Nächste »

Datenschützer verabschieden neues Prüfmodell

heise online 01.10.2015 14:13 Uhr – Christiane Schulzki-Haddouti vorlesen

(Bild: BSI)

Die Datenschutz-Aufsichtsbehörden von Bund und Ländern empfehlen, das Standard-Datenschutzmodell anzuwenden. Dieses unterstützt ein strukturiertes Prüfen von IT-Prozessen, was bisher mangels eines eigenen Prüfmodells nicht möglich war.

- Regelungskern: 7 Schutzziele
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- 3 Schutzbedarfsabstufungen, formuliert aus Betroffenenperspektive
- Referenzkatalog mit Schutzmaßnahmen
- DSB-Konferenz hat SDM-Handbuch (V0.9 /Oktober 2015) angenommen
- Auf der DSB-Konferenz im November soll V1.0 (mit Referenz-Maßnahmenkatalog) erscheinen.

Referenzkatalog mit Schutzmaßnahmen

* **Datensparsamkeit** / Reduzierung erfasstet Attribute betroffener Personen und der Verarbeitungsoptionen / Reduzierung der Möglichkeiten der Kenntnisnahme vorhandener Daten
* **Verfügbarkeit** / Redundanz, Backup und Restore / Vertretungsregeln
* **Integrität** / technischer Integritätsschutz (elektronische Signaturen und deren Prüfungen) / Soll-Definitionen für Prozesse, mit Ereignisdefinitionen zur Prüfbarkeit von Soll-Abweichungen
* **Vertraulichkeit** / Verschlüsselung von Datenbeständen und Kommunikationen / Berechtigungen- & Rollenkonzept
* **Nichtverkettbarkeit** / Trennung / Isolierung unter der inhaltlichen Maßgabe der Umsetzung informationeller Gewaltenteilung / Anonymisierung / Pseudonymisierung
* **Transparenz** / Spezifikation von geplanten Systemen / Dokumentation, die eine Prüffähigkeit von Ist-Zuständen und Soll-Vorgaben erlaubt / Protokollierung von Prozess-Ereignissen / Auskunft
* **Intervenierbarkeit** / Berichtigung, Sperrung, Löschung, Widerspruch („Außenschnittstelle“ einer Organisation) / Prozesse einer Organisation zur Erkennung und Bearbeitungen von Störungen, Problembearbeitungen und Änderungen („Changemanagement“)

Grundsätze für die Datenverarbeitung – Art. 5

Art. 5 Abs. 1 „Personenbezogene Daten müssen“	**Schutzziele:**
(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**).“	**Transparenz**
(b) „... für festgelegte eindeutige und legitime Zwecke erhoben werden ... (**Zweckbindung**).“	**Nicht-Verkettbarkeit**
(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**).“	**Datensparsamkeit**
(d) „... damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ... **unverzüglich gelöscht oder berichtigt** werden.“	**Intervenierbarkeit**
(f) „... **Integrität und Vertraulichkeit**“.	**Integrität und Vertraulichkeit**

Es fehlt: **Verfügbarkeit ???**

Mapping SDM-Schutzziele und DSGVO

Schutz-ziele:	Datenspar-samkeit	Verfügbar-keit	Integrität	Vertraulich-keit	Nichtver-kettbarkeit	Transparenz	Intervenier-barkeit
Artikel der DS-GVO:	5c/e, 25	13, 15, 20, 25, 32	5d,f, 25, 32	5f, 25, 28/3b, 32	5b, 25, 32	5a, 12, 13, 14, 15, 25, 32, 33, 34	12/2, 15e, 16, 17, 18, 19, 20, 21, 22/3, 25, 28/3g

Zweckbindung

Quelle: android-news-blog.de

Artikel 6 Abs. 4 DS-GVO

Zweckänderung („Weiterverarbeitung“) ist nur zulässig nach Prüfung der „Vereinbarkeit“ mit dem ursprünglichen Zweck, insbes. hinsichtlich:

- Verbindung der Zwecke
- Erhebungszusammenhang
- besonderer Daten (Art. 9/9a)
- Folgen der Weiterverarbeitung für Betroffene
- Vorhandensein angemessener Garantien, z. B. Pseudonymisierung, Verschlüsselung

Erwägungsgrund 50 DS-GVO

- Der Maßstab für die Vereinbarkeit sind *„die vernünftigen Erwartungen der betroffenen Person“.*

Transparente Verarbeitung

Artikel 12 DS-GVO
Transparenz und Modalitäten der Verarbeitung

durch Information
(Art. 13, 14 und 34)

- Mitteilungen bei der Erhebung
  - beim Betroffenen
  - nicht beim Betroffenen (im Sinne von Information, Unterrichtung und Aufklärung)
- Benachrichtigung bei Datenpannen

durch Auskunft
(Art. 15)

- Werden Daten verarbeitet?
- Details zur Datenverarbeitung
- Details zur Übermittlung
- Recht auf Kopien

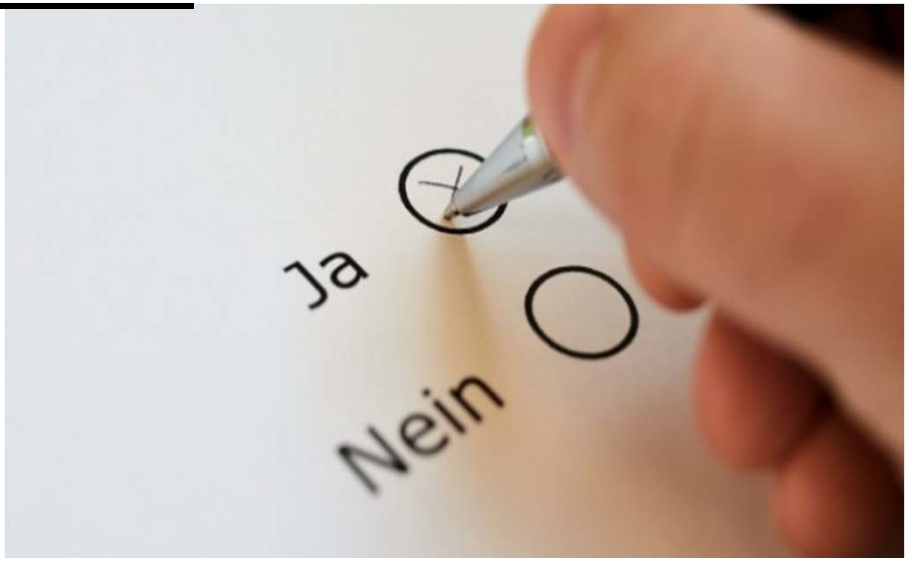
durch Intervention
(Art. 16-21)

- Berichtigung
- Löschung
- Recht auf Vergessenwerden
- Einschränkung der Verarbeitung
- Datenübertragung
- Widerspruch

Einwilligung

Artikel 6 Abs. 1a, 7 und 8 DS-GVO

- freiwillig
- informiert
- konkret
- unmissverständlich
- klar
- kopplungsfrei
- nachweisbar
- einfach und verständlich
- für die Zukunft widerrufbar
- nicht widersprüchlich zur DS-GVO



Art. 8 DS-GVO: Sonderregelung für Kinder:
- nationaler Spielraum für Altersgrenzen: zwischen 13 und 16 Jahren

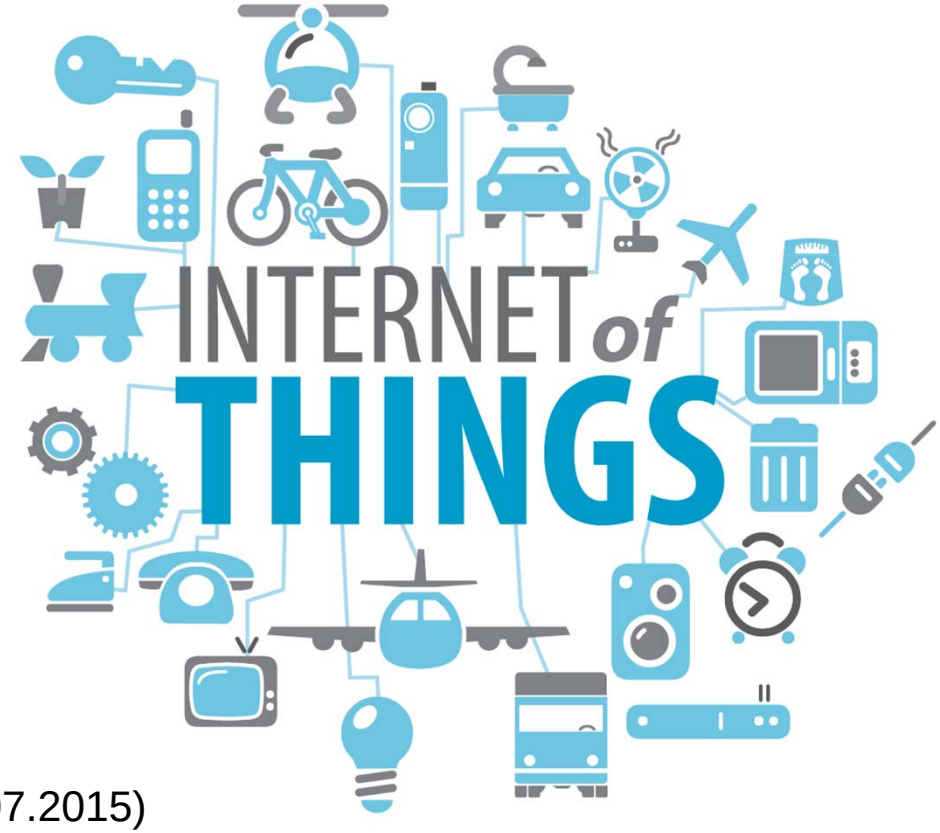
Internet der Dinge

Fakten Fakten Fakten:

Wer kennt:

- Industrie 4.0 = 18%
- „Internet der Dinge“ = 12%
- Paketverfolgung = 80%

- Persönlicher Nutzen <50%



Quelle: Umfrage für Telekom (aus FAZ 28.07.2015)

Quelle: www.engineering.com

Internet der Dinge???

Der *Versuch* einer Definition:

Mark Weiser 1991: „**The Computer for the 21st Century**“

Intelligente Gegenstände („smart things“) ersetzen den Computer und unterstützen ohne aufzufallen oder abzulenken.

„Im 21. Jahrhundert wird die technologische Revolution das Alltägliche, Kleine und Unsichtbare sein.“

Aufgaben von UC-Systeme

- stetig und überall verfügbare Computerunterstützung („ubiquitär“)
- stark vereinfachte Schnittstellen zwischen Mensch und Computer, welche die Aufmerksamkeit und Interaktion der Nutzer minimal einfordern („Calm Computing“)
- automatische Steuerung und Anpassung der Umgebung an Nutzerpräferenzen oder situative Kontexte
- automatische Ausführung und Abwicklung wiederkehrender standardisierter Abläufe ohne Einforderung einer Nutzerinteraktion

Komponenten von UC-Systeme

- verteilte Infrastruktur für Sensoren und Schnittstellen (Interfaces)
- verteilte Infrastruktur für Transport von Daten
- Rechenleistung von einem oder mehreren (verteilten) Computern, die Daten verarbeiten und Entscheidungen treffen
- Zugriff auf einen oder mehrere (verteilte) Datenspeicher
- Anbindung an externe Datenquellen und Dienste
- Komponenten zur Umsetzung von Entscheidungen bzw. zur Ausführung einer Dienstleistung (Service) oder anderen Aktionen, ggf. auch in einer verteilten Infrastruktur

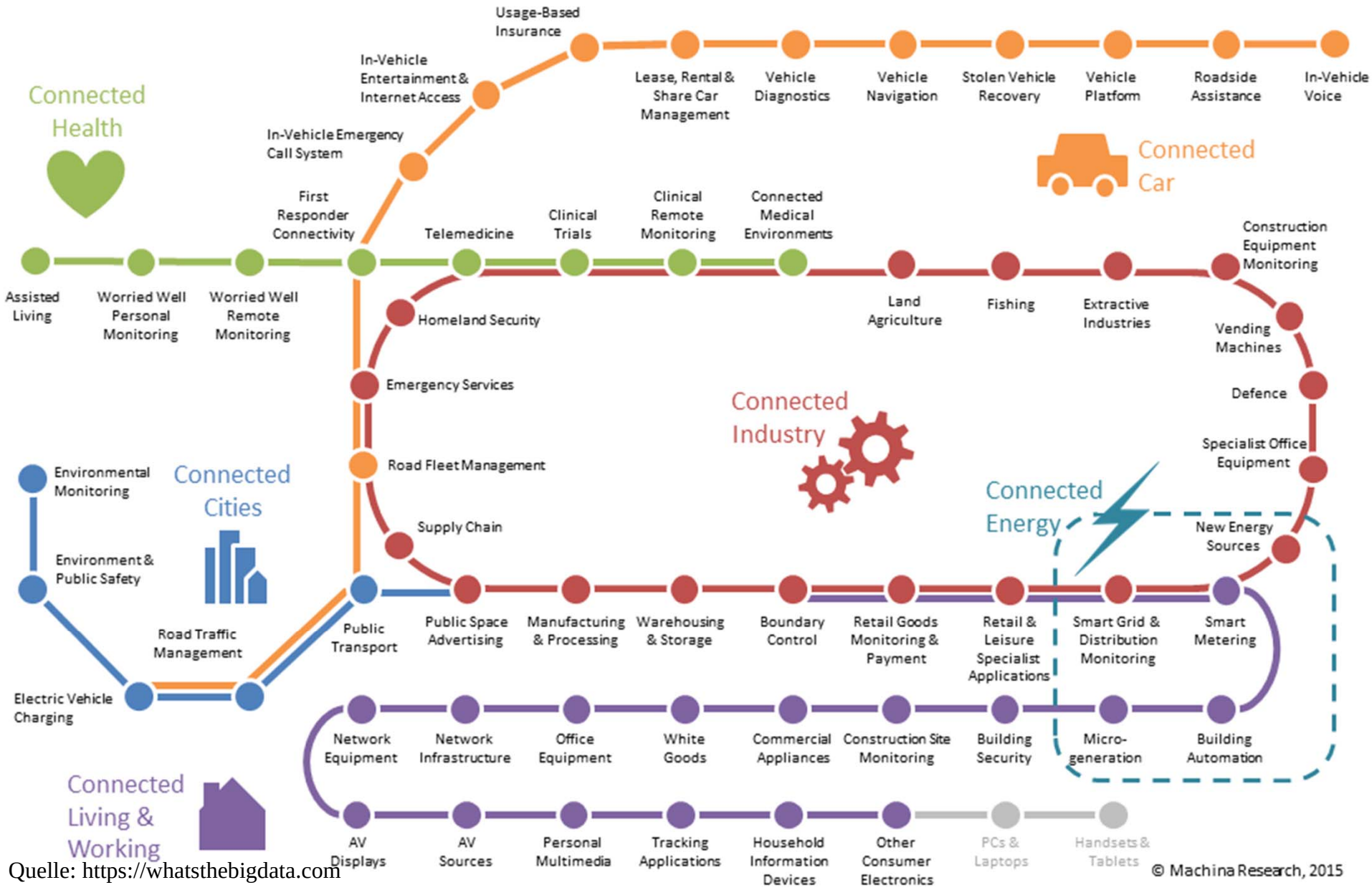
Datenschutz bei UC

Vorhersagen von Mark Weiser:

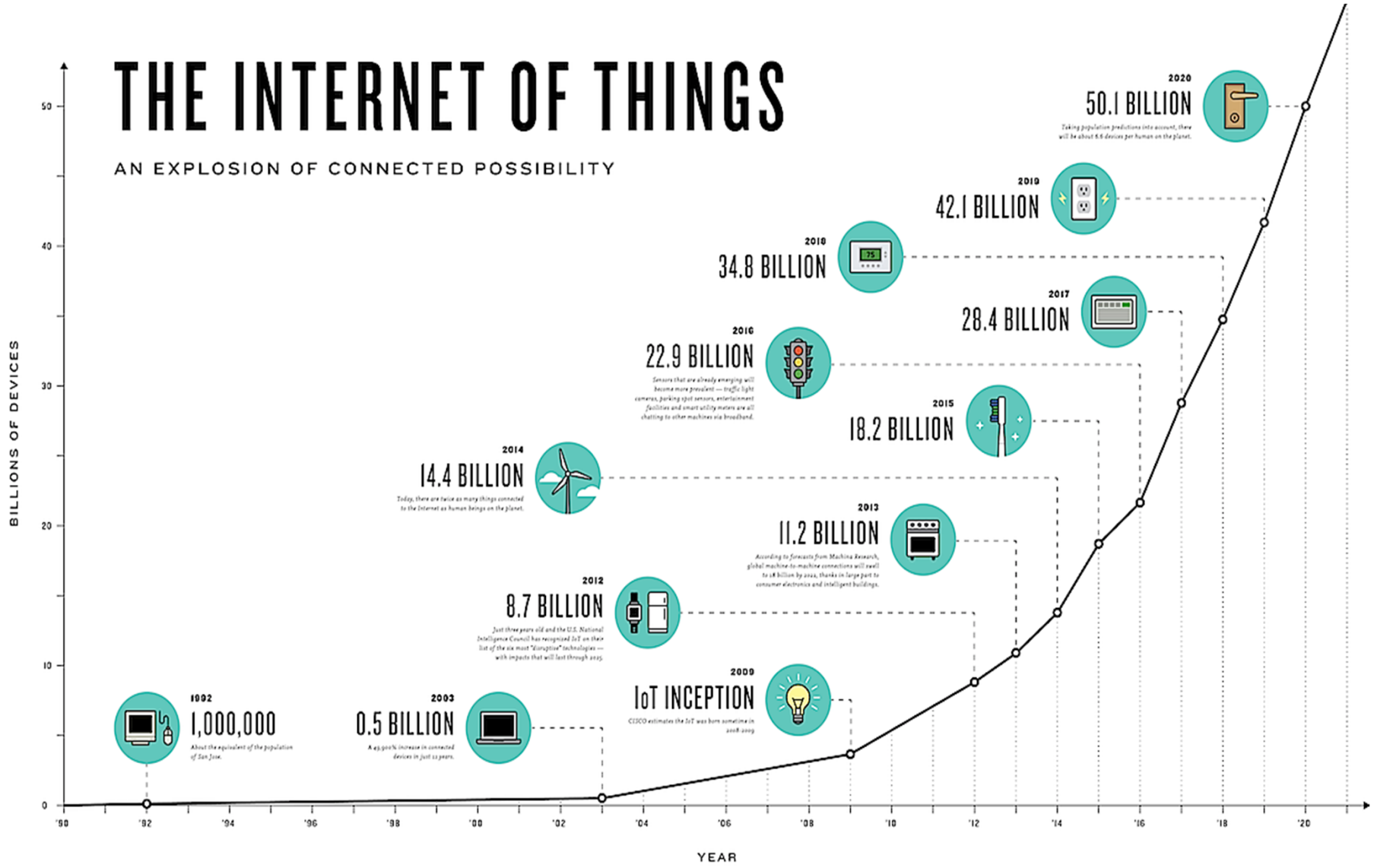
- ReceptionistIn weiß jederzeit wo sich Leute befinden, Terminals wissen wer vor ihnen sitzt und kennen die Präferenzen, Kalender schreiben sich selbst
- 100erte Computer in einem Raum: Gefahr von totalitärem System
- Regierung und Marketingfirmen nutzen Informationen
- better Privacy durch „digital pseudonyms“
- „build computer systems to have the same privacy safeguards as the real world…“

von UC zu IoT

- 1999: Kevin Ashton „begründet“ Begriff „Internet of Things“ in Präsentation bei Procter & Gamble
- ab ‘99: Auto-ID Center am Massachusetts Institute of Technology (MIT) entwirft firmenübergreifende RFID-Infrastruktur
- Mitgründer und damaliger Leiter Kevin Ashton wird 2002 im Forbes Magazine mit „we need an internet for things, a standardized way for computers to understand the real world“ zitiert



Quelle: https://whatsthebigdata.com



http://www.i-scoop.eu/internet-of-things/

Beispiele für IoT Geräte und Anwendungen

- RFID, WLAN, Bluetooth und Co.

Problem: für Lesen der Kennung kein Sichtkontakt notwendig: WWW: Wann und Wo und *Was* wird gescannt?

(ebenfalls problematisch: WLAN und Bluetooth)

- Fahrzeugkontrollsysteme

Luftdruck, Abstandsmessung, Helligkeit, Temperatur, Müdigkeitserkennung, Route, Fahrverhalten…

Verwundbare Autos

Wie zwei Hacker einen Jeep übernehmen

Mulmig war dem Journalisten Andy Greenberg, als sein Auto bei 110 Stundenkilometern gehackt wurde. Wenigstens wusste er grob, worauf er sich einlässt. Doch Besitzer smarter Autos dürften Bauchschmerzen bekommen.

22.07.2015, von FRIDTJOF KÜCHEMANN

© DPA

Da hilft nur noch beten: Die elektronische Ausstattung macht den Jeep Cherokee attraktiv - und angreifbar.

Quelle: FAZ.net

Beispiele für IoT Geräte und Anwendungen

- Digitale Selbstvermessung „Quantified Self“/Smart Health

  Life-Logging (Wearables): sportliche Leistung, Schlaftracking, Gesundheitszustand,…

  - Adidas kauft Runtatstic für 220 Million € (70 Millionen Nutzer; Fitbit beim Börsenstart 6 Mrd $ wert)
  - HealthGraph-Daten (7 Mio. Nutzer) werden für Forschung verwendet; Angaben zu Forschungszweck und ob Anonymisierung: ???
  - Runtastic: Datenverwendung „im Rahmen einer *sonstigen Aktivität* von Runtastic oder einem mit Runtastic verbundenen Unternehmen“ und „Recht der Veränderung und Bearbeitung, sofern nicht dadurch *berechtigte Interessen des Nutzers* beeinträchtigt werden“

Beispiele für IoT Geräte und Anwendungen

- Smart Home / Smart Living

Vernetzung von Haustechnik, Haushaltsgeräten und Unterhaltungselektronik

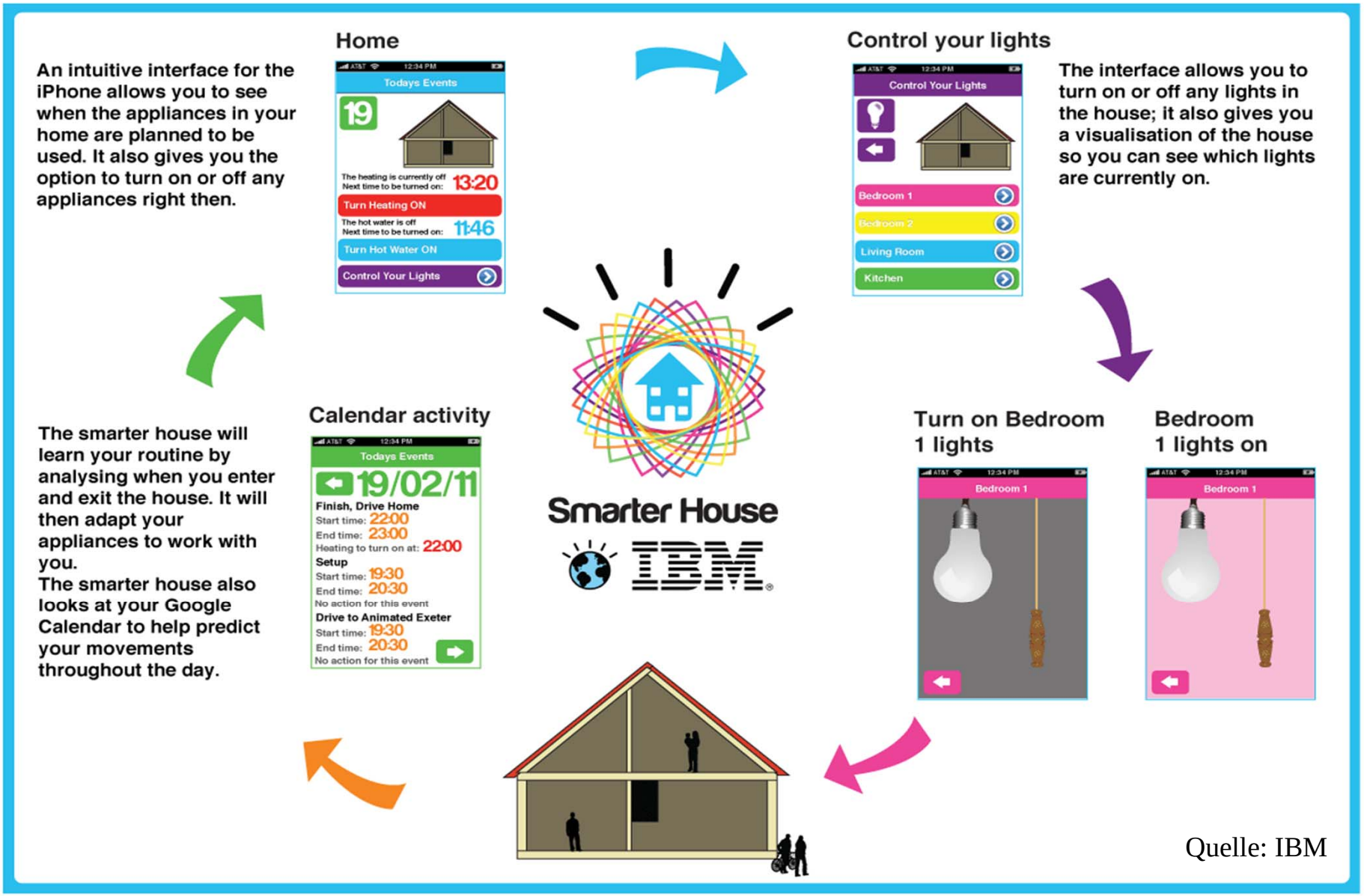
- Smart Metering

„Intelligenter Zähler“ zum digitalen messen und steuern von Energie-, Wasser- und Gasverbrauch

KNX: Europäischer Installationsbus

Quelle: www.silchinger.de

Was ist ein intelligentes Gebäude?



Quelle: IBM

Smart Home: Hacker übernehmen Kontrolle über Thermostat

heise online 09.08.2016 19:32 Uhr – Volker Briegleb vorlesen

Dieses Thermostat heizt nur noch gegen Bitcoin. (Bild: Ken Munro auf Twitter)

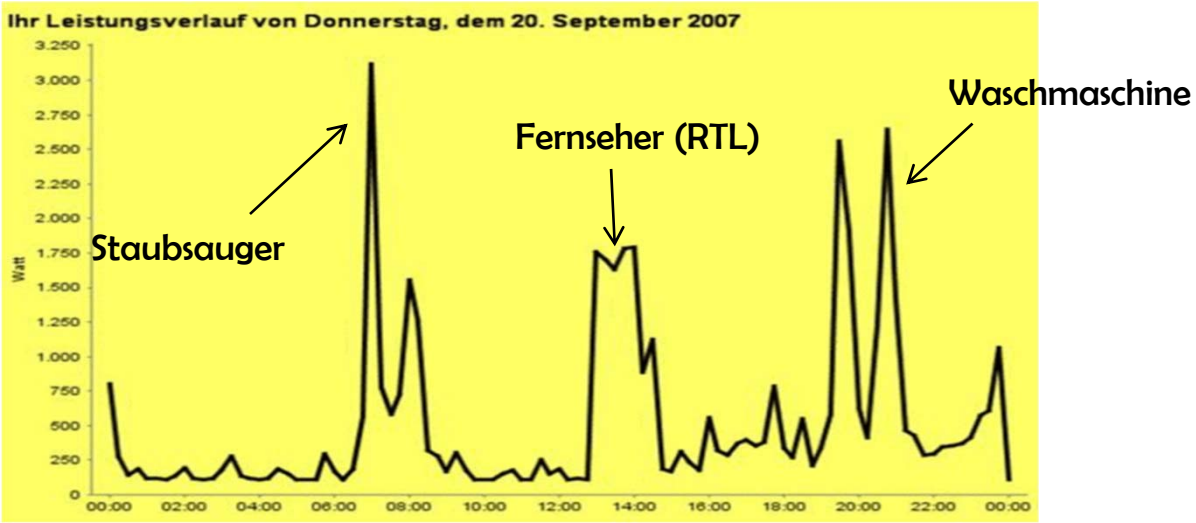
Die Sicherheitsexperten Andrew Tierney und Ken Munro haben auf der Hacker-Konferenz Def Con gezeigt, wie sie ein "smartes" Thermostat kapern können. Wirklich schwer hat es ihnen die Hardware dabei nicht gemacht.

Auf der Hacker-Konferenz Def Con 24 in Las Vegas haben zwei Sicherheitsexperten gezeigt, wie sie ein vernetztes Thermostat eines ungenannten Herstellers mit einer Erpressungs-Software infizieren konnten. Den Hackern ist es gelungen, die Kontrolle über das Thermostat zu erlangen und die Funktionen für den Besitzer zu sperren. Theoretisch könnten Angreifer so zum Beispiel im Winter die Heizung abstellen, bis der arme Wohnungsinhaber zahlt.

"Armselige Sicherheit"

Quelle: Heise.de

Smart Meter



- differenzierte Verbrauchsmessung elektrischer Geräte
- eine Überwachung defekter elektrischer Geräte ("Pre-Maintenance")
- Zugriff auf einzelne elektrische Geräte auch aus der Ferne ("Remote Access")

Diese Informationen sind personenbezogen!

Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

PRESSEMITTEILUNG 22. September 2016

Datenschutz beim „Internet der Dinge“ – Klein und nicht fein!

Unter dem Titel „GPEN Privacy Sweep 2016“ hat die englische Datenschutzaufsichtsbehörde eine Aktion zur Prüfung des Datenschutzes bei Produkten im Bereich des „Internet der Dinge“ bzw. „Internet of Things“ (IoT) angestoßen und koordiniert. GPEN steht für „Global Privacy Enforcement Network“ und ist ein informeller Zusammenschluss von Datenschutzaufsichtsbehörden auf der ganzen Welt. An der diesjährigen Prüfung haben 25 der im GPEN aktiven Datenschutzaufsichtsbehörden teilgenommen. Auch der Landesbeauftragte für den Datenschutz Baden-Württemberg hat sich an der Aktion beteiligt und Produkte untersucht, die in Baden-Württemberg entwickelt werden.

Immer mehr elektronische Produkte sind heutzutage mit dem Internet verbunden - von Steuergeräten für das „Smart Home“ über Fitness Tracker oder Pulsmesser bis hin zum Smart TV. Dank miniaturisierter Sensoren wird eine Vielzahl physikalischer oder biomedizinischer Größen durch diese „intelligenten“ Geräte erfasst. Gesteuert werden sie häufig per App auf dem Smartphone. So lässt sich beispielsweise die Heizung im Smart Home von überall auf der Welt per App ein- und ausschalten. Auch

Fazit

(Kurz-)Fazit

- DPIA – Data Protection Privacy Assessment (Art. 35 DSGVO)
- Privacy by Design und Privacy by Default (Art. 25)
- Datenminimierung: so wenig Daten wie nötig, Rohdaten frühestmöglich und am dichtesten Punkt (am „Smart Device“) löschen, Daten aggregieren wenn möglich (Art. 5)
- Einsatz verschlüsselter Kommunikation; ggf. Entwicklung neuer Verschlüsselungsalgorithmen notwendig
- nutzerfreundliche Informationspflichten / Einwilligungen (Art. 7)
- feingranulare „Datensteuerung“ ermöglichen (opt-out und abschalten von einzelnen Funktionen)
- Zertifizierung und Auditierung von Produkten und Verfahren (Art. 42)
- Data Breach Notifications (Infos über Datenlecks und Anleitungen) (Art. 34)

ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 223

Opinion 8/2014 on the on Recent Developments on the Internet of Things

Adopted on 16 September 2014

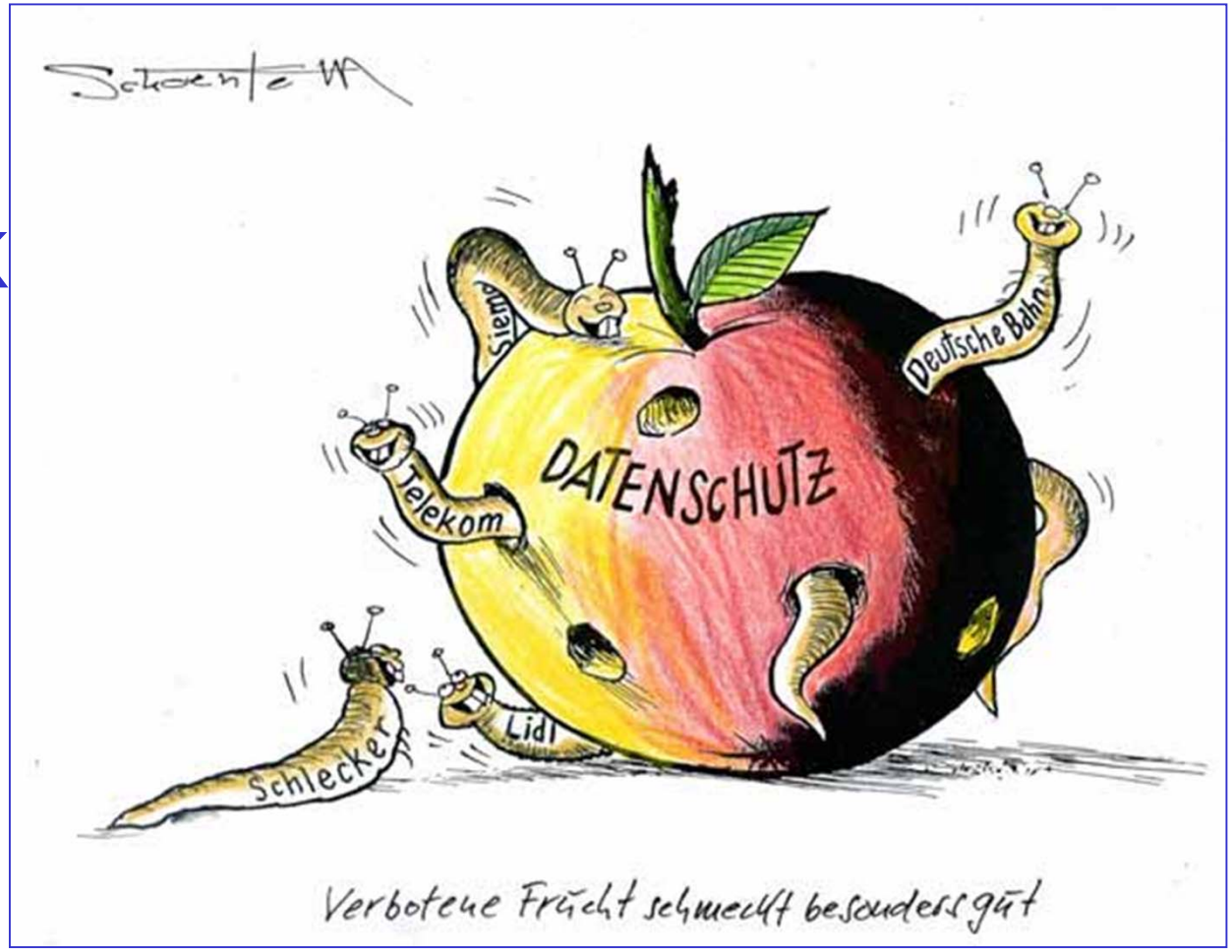
Orientierungshilfe – Cloud Computing

der Arbeitskreise Technik und Medien
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises

Version 2.0
Stand 09.10.2014

DÜSSELDORFER KREIS
Aufsichtsbehörden für
den Datenschutz im
nicht-öffentlichen Bereich

Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter

Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich.

Vielen Dank für Ihre Geduld!