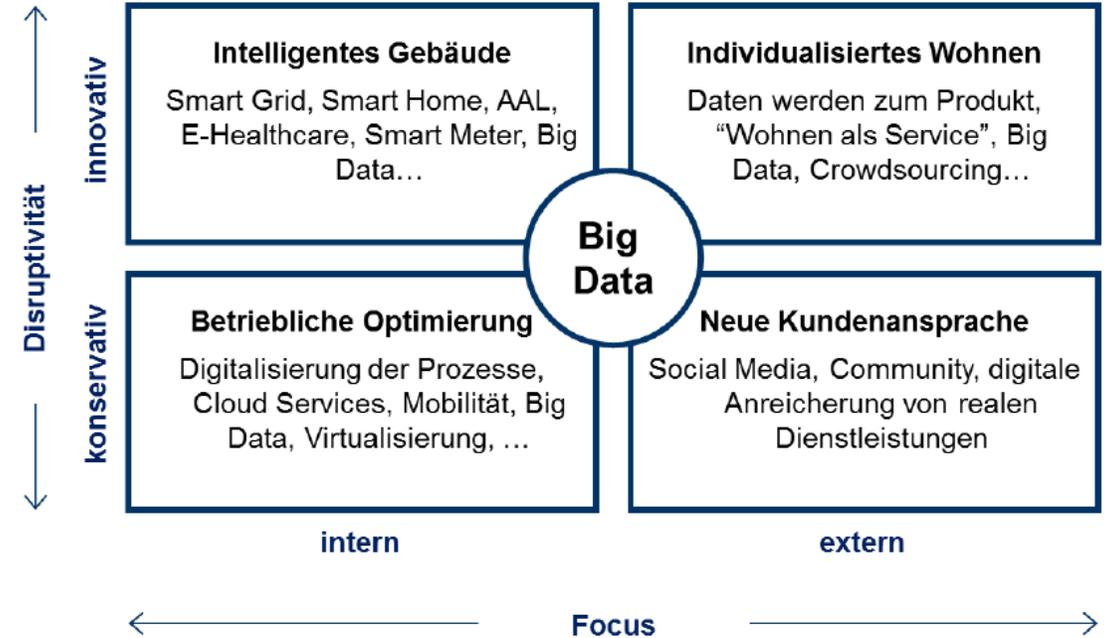
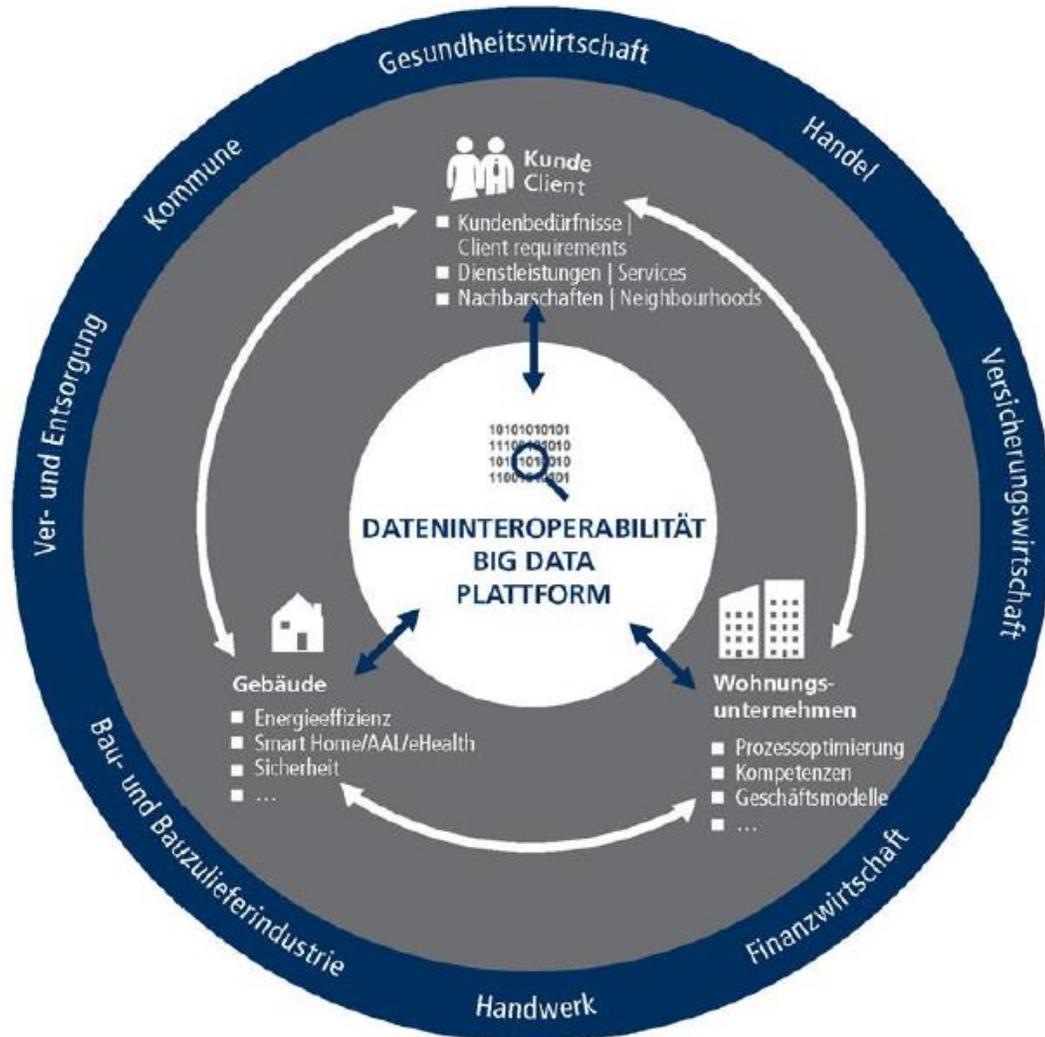




# Public Key Infrastructure, Messstellenbetrieb, Common Criteria, TR 03109, DSGVO und die Folgen: Was kommt auf anwendende Betriebe zu?

Dr.-Ing. Lutz Martiny  
achelos GmbH, Paderborn  
Leiter KF 5 Green with IT  
Berlin, 01. März 2018

# Digitalisierung als durchgehende Vernetzung mit allen Akteuren



Quelle: InWis Studie Digitalisierung in der Immobilienwirtschaft – Chancen und Risiken, 2016 S. 8

## ABER:

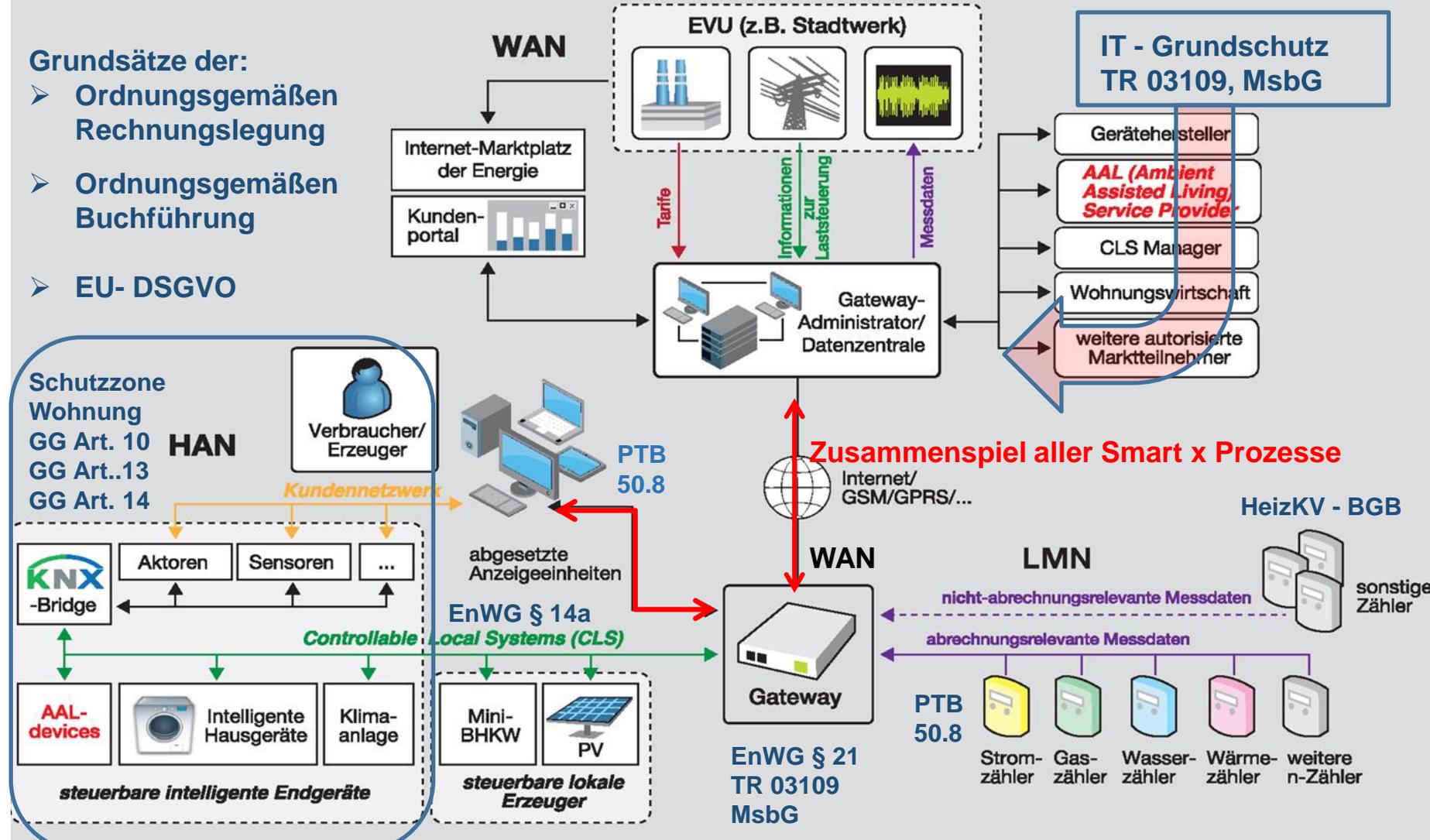
es gelten eine Vielzahl von Gesetzen und Verordnungen **für alle Marktteilnehmer**, um die Anforderungen an Datenschutz, Datensicherheit und Interoperabilität zu erfüllen, die bei Nichteinhaltung z.T. strafbewährt sind.

Quelle: InWis Digitalisierung in der Immobilienwirtschaft, Studie 2016, Seite 16

# Datenschutz- und Sicherheit: technisch-regulatorischer Rahmen

Grundsätze der:

- Ordnungsgemäßen Rechnungslegung
- Ordnungsgemäßen Buchführung
- EU- DSGVO



**EU-DSGVO** europäische Datenschutzgrundverordnung

**WAN** wide area network ("Internet")

**HAN** home area network ("Heimnetzwerk")

**LMN** local metrological network (lokales Netzwerk zum Messen)

**Smart Meter** Zähler messen elektronisch, leiten Daten an das Gateway

**CLS** Controllable-Local-System baut gesicherte Verbindungen zu Externen per WAN auf.

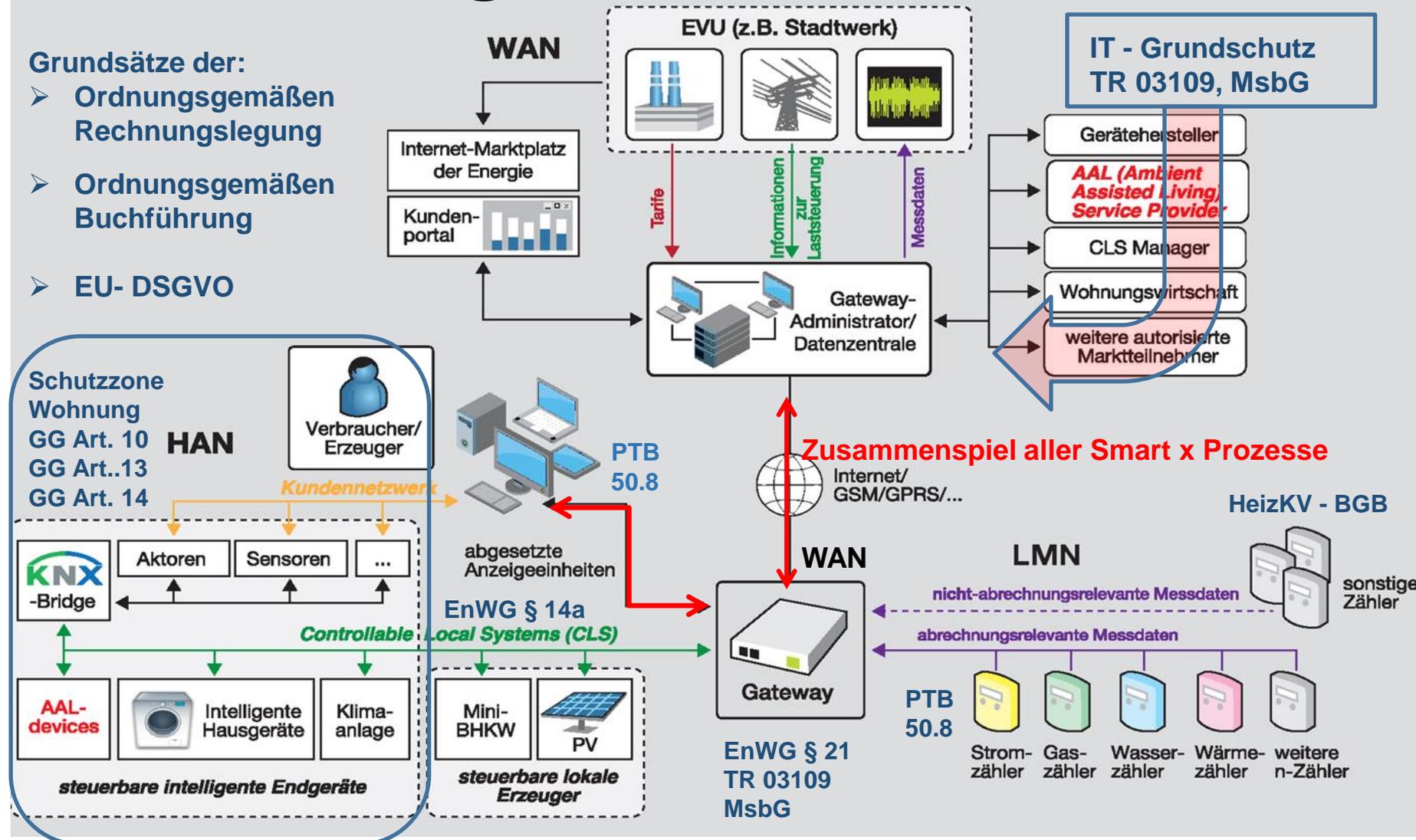
**Gateway-Administrator** entscheidet, wer wann welche Daten erhält.

**MsbG** Messstellenbetriebsgesetz  
**PTB 50.8** eichrechtliche Anforderungen

# Datenschutz- und Sicherheit: technisch-regulatorischer Rahmen

Grundsätze der:

- Ordnungsgemäßen Rechnungslegung
- Ordnungsgemäßen Buchführung
- EU- DSGVO

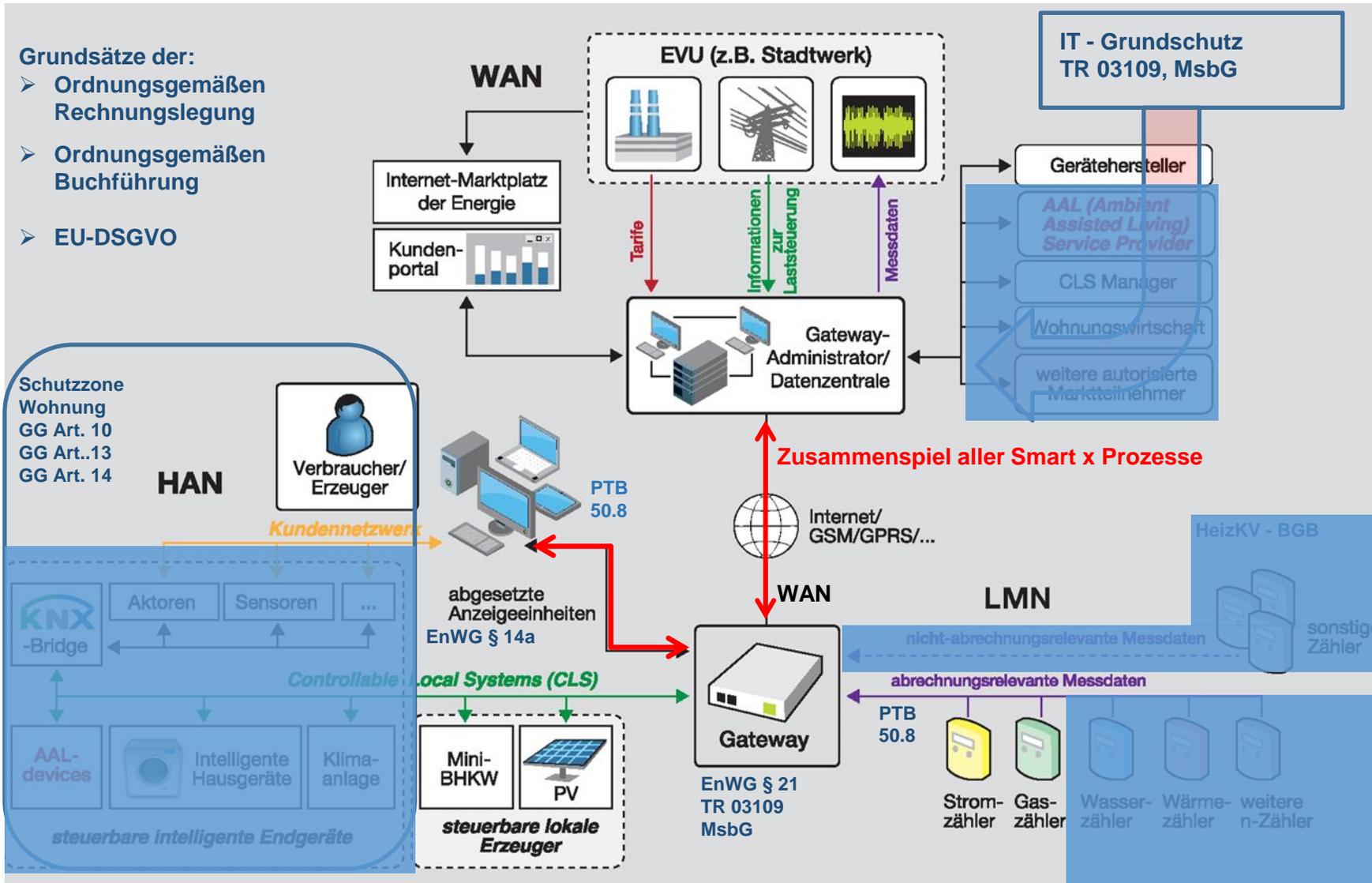


Hyper Complexity  
+ Hyper Connectivity  
+ Hyper Data Volumes

= **Hyper Vulnerability**

Quelle: Transformational 'smart cities': cyber security and resilience-  
Symantec Executive Report 2013, Seite 10

# Relevanz für die Energiewirtschaft



## Messstellenbetriebsgesetz Ziel:

- Funktionssicherheit durch Zertifizierung nach Common Criteria
- Datensicherheit
- Interoperabilität
- Übertragungssicherheit - -- Zuordnung der Verantwortung
- Datenschutz

# Was müssen Unternehmen tun?

## 1) Versorgungsnetzbetreiber

Betreiber von Energieversorgungsnetzen müssen eine zentrale Entscheidung gleich am Anfang des Prozesses treffen: In welchem Umfang sie die mit der „Digitalisierung der Energiewende“ verbundenen Aufgaben an externe Dienstleister übergeben wollen – sei es ganz oder teilweise, vorübergehend oder dauerhaft. Hier sind verschiedene Varianten denkbar.

Bei der Übertragung der „Grundzuständigkeit“, bei der ein anderes Unternehmen die wesentlichen Aufgaben des Messstellenbetriebs übernimmt, ist – wenn keine Ausnahme greift – ein Vergabeverfahren durchzuführen. Es kommt in einem solchen Verfahren dann einerseits auf die Beachtung der allgemeinen vergaberechtlichen Vorschriften an. Andererseits stellen die §§ 41 ff. MsbG an die Übertragung der „Grundzuständigkeit“ auch besondere zusätzliche vergaberechtlich relevante Anforderungen.

## 2) Dienstleister und Gerätehersteller

Unternehmen, die Unterstützungsleistungen für Smart Meter und moderne Messeinrichtungen anbieten wollen, können sich auf Basis des nun final vorliegenden Gesetzestextes auf die regulatorischen Anforderungen einstellen. Insbesondere ist das für Unternehmen notwendig, deren Unterstützungsleistungen in den Bereich einer der im Gesetz fest definierten „Rollen“ fällt (insb. die Rollen des ‚Messstellenbetreibers‘ und des ‚Smart Meter Gateway Administrators‘). Aber auch die eingesetzte Hardware muss genau definierten rechtlichen und technischen Anforderungen genügen; vor der Verwendung muss sie **vom BSI zertifiziert werden**.

## 3) Telekommunikationsdiensteanbieter

Für Anbieter von Telekommunikationsdiensten, die die Smart Meter-Infrastruktur vernetzen wollen, ist zunächst einmal wichtig, dass das MsbG **technologieneutral** ausgestaltet ist. Es kommen also unterschiedliche Technologien in Frage.

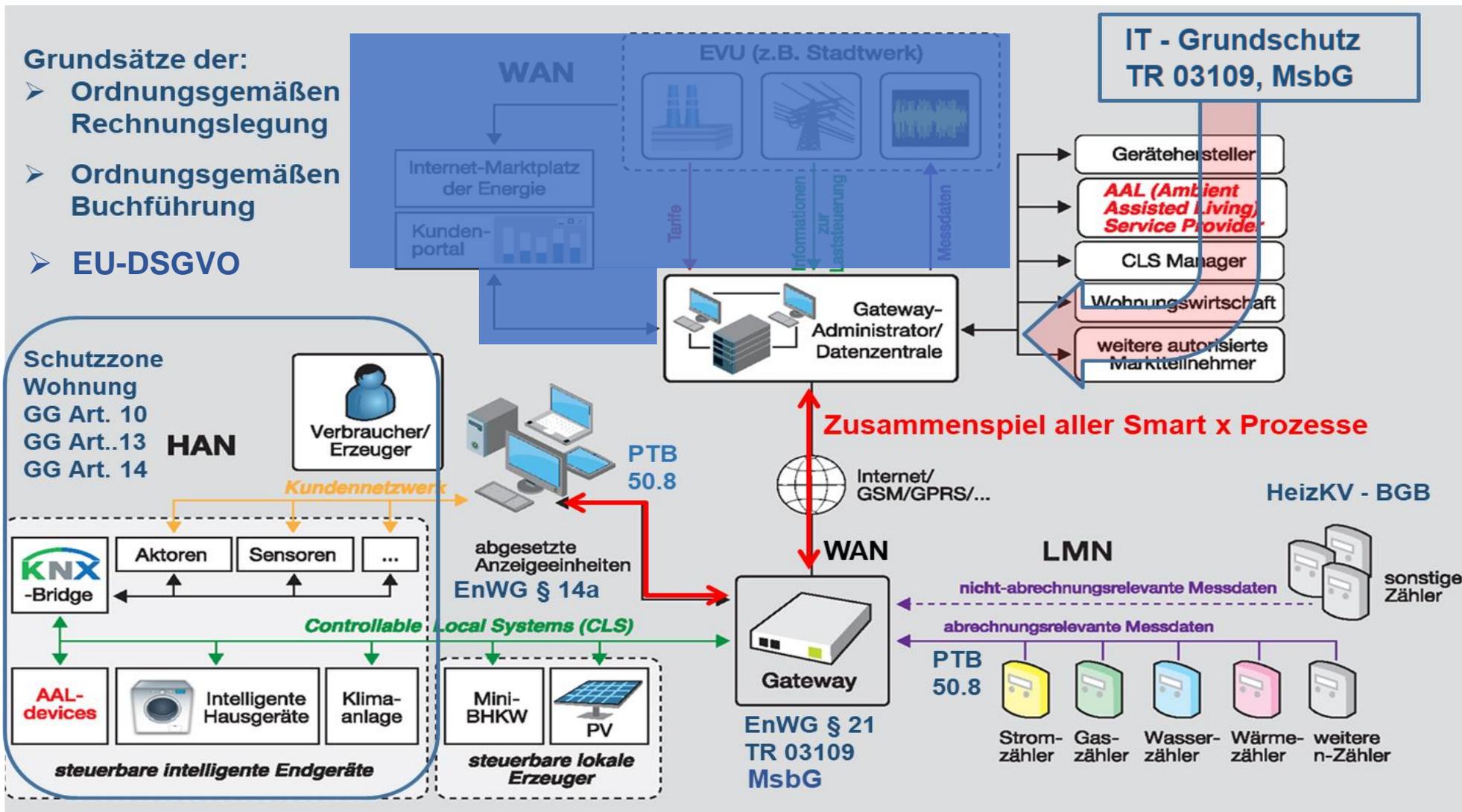
Telekommunikationsdienste, die für die neue Smart Meter-Infrastruktur genutzt werden sollen, müssen allerdings regulatorische Vorgaben beachten, u.a. zur Zuverlässigkeit und Leistungsfähigkeit (§ 25 Abs. 2 MsbG) und zur Übertragungssicherheit (§ 21 Abs. 1 Nr. 3 MsbG). Die Anforderungen können vom BSI und der Bundesnetzagentur auch nachträglich noch spezifiziert werden (§ 22; § 27; § 47 Abs. 1 Nr. 3; § 75 Nr. 1 MsbG). Das BSI stellt auf seiner Webseite eine Übersicht über seine bisherigen Anforderungen zur Verfügung.

Quelle: <https://www.twobirds.com/de/news/articles/2016/germany/july/germany-launches-smart-metering-roll-out>

# Relevanz für die Wohnungswirtschaft

Grundsätze der:

- Ordnungsgemäßen Rechnungslegung
- Ordnungsgemäßen Buchführung
- EU-DSGVO



Auswirkungen auf:

- Unternehmen der Wohnungswirtschaft
- Kunden (Mieter)
- Gebäude

Quelle: nach Uhlig, R., weolution, Omnicard 2015

# Interoperabilität: Smart Home Standards ?

Welche Systeme passen zusammen (Eine Auswahl)

Belkin WeMo | Bosch SmartHome

Elgato Eve | Gigaset Elements

HomeMatic | HomeMatic IP

Loxone | Magenta Smart Home

Microsoft Home Hub

Samsung SmartThings

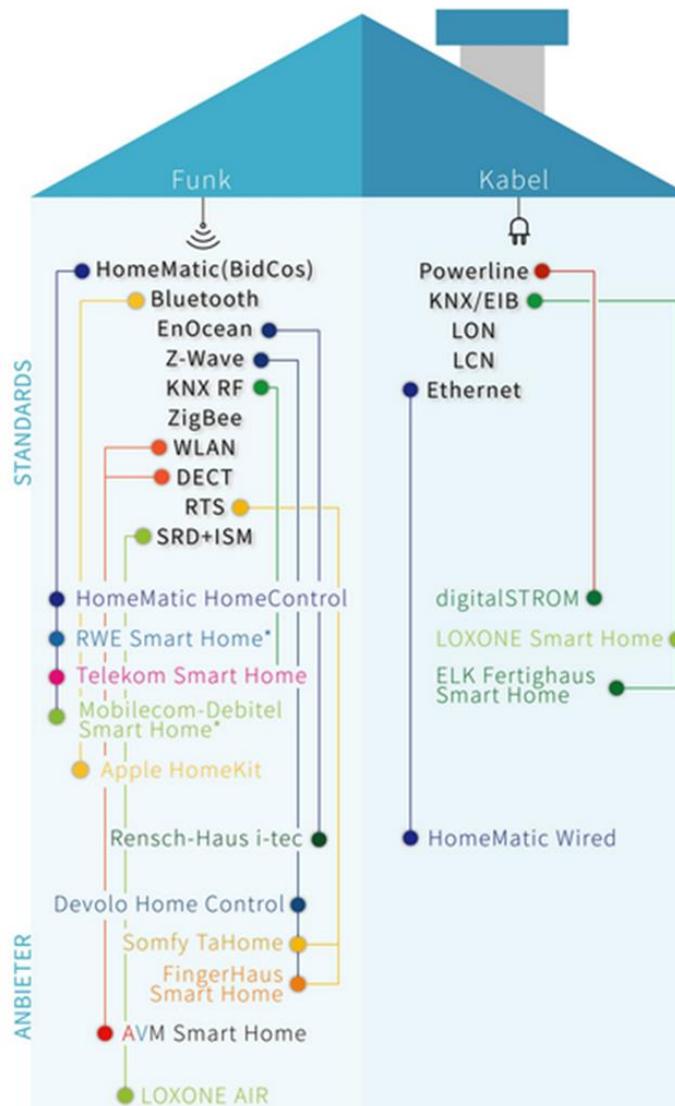
TaHoma Connect

Zipato Smart Home

devolo Home Control

digitalSTROM | innogy SmartHome

mydlink Home | Qivicon



## Smart Home Anbieter-Kompatibilität

Telekom Smart Home + RWE Smart Home = X

Apple HomeKit + Telekom Smart Home = X

Telekom Smart Home + HomeMatic = ✓

HAUSXXL

Ihr Bauratgeber - Kostenlos & Regional

Quelle: <http://www.haus-xxl.de/themen/smart-home-standards-was-steht-hinter-den-marketingbegriffen-481>  
zuletzt besucht am 23.02.2018

# Qivicon: Ein Standard?

## QIVICON HOME BASE APPS, MIT DENEN SIE IHR SMART HOME KONTROLLIEREN UND STEuern KÖNNEN:



TELEKOM MAGENTA SMARHTHOME



MIELE STARTUP CONNECT



E WIE EINFACH EinfachSmart-App



RHEINENERGIE SMART HOME



VATTENFALL SMART HOME MANAGER



ENTEKA SMART HOME



LOGITECH HARMONY



SWB-SmartHome App



EWV SMART HOME

# Sicherheit steuerbarer intelligenter Endgeräte in Analogie zu den Erfordernissen des IT-Grundschutz, TR 03109, MsbG

Grundsätze der:

- Ordnungsgemäßen Rechnungslegung
- Ordnungsgemäßen Buchführung
- EU-DSGVO

Analogie zu IT – Grundschutz TR 03109, MsbG

Schutzzone Wohnung  
GG Art. 10  
GG Art. 13  
GG Art. 14

HAN



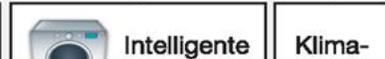
abgesetzte Anzeigeeinheiten

Kundennetzwerk



Controllable Local Systems (CLS)

AAL-devices



steuerbare intelligente Endgeräte

EnWG § 14a

steuerbare lokale Erzeuger



EnWG § 21 TR 03109 MsbG

Gateway

WAN



Internet/ GSM/GPRS/...

WAN

Internet-Marktplatz der Energie

Kundenportal

EVU (z.B. Stadtwerk)



Administrator/  
Datenzentrale

IT - Grundschutz TR 03109, MsbG

Gerätehersteller

AAL (Ambient Assisted Living) Service Provider

CLS Manager

Wohnungswirtschaft

weitere autorisierte Marktteilnehmer

Zusammenspiel aller Smart x Prozesse

HeizKV - BGB

LMN

nicht-abrechnungsrelevante Messdaten

abrechnungsrelevante Messdaten

PTB 50.8

Strom-zähler

Gas-zähler

Wasser-zähler

Wärme-zähler

weitere n-Zähler

sonstige Zähler

# Sicherheit und Datenschutz im Smart Home

## Funktionssicherheit:

unter Funktionssicherheit wird im Wesentlichen der Schutz vor unbeabsichtigten Ereignissen verstanden. "Smart" wird das SmartHome überhaupt erst, wenn die Technik nicht nur funktioniert, sondern auch dafür sorgt, dass sie **wieder** funktioniert, wenn sie **nicht** funktioniert hat.

## Informationssicherheit

Angriffspunkte/Ziele Verfügbarkeit, Vertraulichkeit, Authentizität, Integrität, Privatsphäre

**Datenschutz (ab 25. Mai 2018 nach EU-Recht für alle in der EU ansässigen Unternehmen gilt die Datenschutz Grundverordnung, DSGVO) mit den Grundsätzen „Privacy by Design“ und „Privacy by Default“**

**Verbot mit Erlaubnisvorbehalt:** Es dürfen keine personenbezogenen Daten erhoben werden, außer es gibt eine Einwilligung des Betroffenen.

**Grundsatz der Datensparsamkeit:** Es sollen so wenig Daten wie möglich gesammelt werden.

**Grundsatz der Erforderlichkeit:** Es sollen nur die Daten, die benötigt werden, erhoben werden.

**Grundsatz der Zweckbindung:** Der Verwendungszweck der erhobenen Daten muss präzise definiert sein. Die Daten dürfen für keine anderen Zwecke verwendet werden.

**Grundsatz der Transparenz:** Es muss nachvollziehbar sein, wofür die Daten benötigt werden.

**Nichteinhaltung:** Bußgelder in Höhe von bis zu 20 Millionen Euro oder 4% des jährlichen Weltumsatzes, je nachdem, welcher Betrag höher ist.

# Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(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“**);

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“**).

# Art. 7 DSGVO: Bedingungen für die Einwilligung

- Zustimmung unterliegt zusätzlichen Bedingungen der DSGVO.
- Zusätzliche Anforderungen beinhalten ein ausdrückliches Zustimmungsverbot und Angebot von Leistungen, die von der Zustimmung zur Verarbeitung von Daten abhängig sind
- Einwilligung muss übersichtlich dargestellt und getrennt sein von anderen schriftlichen Vereinbarungen, und so leicht zu widerrufen sein wie die Zustimmung erteilt werden kann.
- Für Kinder gelten besondere Regeln für Dienstleistungen der Informationsgesellschaft.

- Stellen Sie sicher, dass Sie sich über die von Ihrer Organisation geltend gemachten Gründe für die rechtmäßige Verarbeitung im Klaren sind, und prüfen Sie, ob diese Gründe im Rahmen der DSGVO weiterhin gelten (siehe Abschnitt über die Rechtmäßigkeit der Verarbeitung und Weiterverarbeitung).
- Überlegen Sie, ob Sie die Regeln für Kinder im Internet betreffen und welche nationalen Regeln Sie wann bei der Einholung der Einwilligung befolgen müssen (siehe Abschnitt über Kinder für weitere Details in Artikel 8 DSGVO).
- Wenn sich Ihre Organisation auf die Einwilligung zur Verarbeitung personenbezogener Daten zum Zwecke der wissenschaftlichen Forschung verlässt, sollten Sie in Erwägung ziehen, betroffenen Personen die Möglichkeit zu geben, nur bestimmten Bereichen der Forschung oder Teilen von Forschungsprojekten zuzustimmen.
- Wenn Sie sich auf die Zustimmung als Grundlage für eine rechtmäßige Verarbeitung verlassen, stellen Sie sicher, dass:
  - \* Die Einwilligung aktiv erfolgt und nicht auf Schweigen, Inaktivität oder vorher angekreuzten Kästchen beruht;
  - \* die Zustimmung zur Verarbeitung klar unterscheidbar ist und nicht mit anderen schriftlichen Vereinbarungen oder Erklärungen "gebündelt" wird;
  - \* die Erbringung von Dienstleistungen nicht von der Zustimmung zur Verarbeitung abhängig gemacht wird, die für die Erbringung der Dienstleistung nicht notwendig ist;
  - \* Betroffene Personen darüber informiert werden, dass sie zu jeder Zeit ein Rücktrittsrecht haben, dass dies aber nicht die Rechtmäßigkeit der Verarbeitung auf der Grundlage der Zustimmung vor seinem Rücktritt beeinträchtigt;
  - \* Sie den Widerruf der Einwilligung so einfach und mit dem gleichen Medium gestalten das Sie für die Einholung der Einwilligung verwendet haben;
  - \* separate Einwilligungen für unterschiedliche Verarbeitungsvorgänge notwendig sind.

# Handlungsbedarf für die Wohnungswirtschaft – oder: Digitalisierung als technische, wirtschaftliche und gesellschaftliche Veränderung begreifen

- Wohnungswirtschaft-interne Klärung strafrechtlicher Relevanz für Vorstände und GF nach Einführung DSGVO (v.a. **Behandlung HKV-Daten** der Mieter)
- Anpassung der IT-Sicherheit: Ableitung eines Anforderungskatalogs für Datenschutz und -sicherheit für die Wohnungswirtschaft, Architekten und Bauunternehmen, die in der Wohnungswirtschaft tätig sind
- Bestellung eines Datenschutzbeauftragten auch zur externen Vertretung gegenüber Behörde
- Nachweispflichten - to do´s
- Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepte
- Anpassung der Dienstleistungsbeziehungen
- Datenschutz „by Design/Default“
- Datenschutz-Folgeabschätzung (DSFA)
- Ausrüstung Reaktionsmechanismen auf Datenverlust
- Evaluierung der Chancen für Mehrwertdienste, die sich aus dem MsbG ergeben (Messtellenbetrieb, Submetering, Mieterstrom ...)
- Aufbau einer Systemplattform für Mehrwertdienste mit den neuen Werkzeugen

# Handlungsbedarf für die Wohnungswirtschaft – Nützliche Links

<http://green-with-it.com/2018/02/15/bbu-neue-informationen-zur-umsetzung-der-datenschutz-grundverordnung/>

[2018-02-06\\_gdw\\_rs\\_datenschutzgrundverordnung - informationen ueber erste anlage 1\\_gdw-musterwohnmandant wohnungsvergabeinteressentenverwaltung](#)  
[anlage 2 fragebogen fuer mietinteressenten](#)  
[anlage 3 informationsblatt mietinteressenten](#)  
[GDD-Praxishilfe DS-GVO 5](#)

<http://green-with-it.com/2018/02/15/grundlagenveranstaltung-des-bbu-zum-thema-dgsvo-in-der-wohnungswirtschaft/>

[1 ueberblick gesetzgebungs-und vo-verfahren mueller-1](#)  
[2 datenschutzbeauftragte batras](#)  
[3 dsgvo-compliance batras](#)  
[4 beschaefigtendatenschutz will](#)



# Vielen Dank für Ihre Aufmerksamkeit

**Dr.-Ing. Lutz Martiny**

achelos GmbH  
Vattmannstraße 1  
33100 Paderborn

Tel.: +49 5251 14212-310  
Mobil: +49 171 5031791

[lutz.martiny@achelos.de](mailto:lutz.martiny@achelos.de)  
[www.achelos.de](http://www.achelos.de)