Berlin, im Juli 2012
Stellungnahme Nr. 65/2012

abrufbar unter
www.anwaltverein.de

Stellungnahme des Deutschen Anwaltvereins

durch den Ausschuss Informationsrecht

zur Konsultation der Europäischen Kommission

The Internet is gearing up for the next technological revolution: communication with and among objects. How would you envisage the "governance" of such an "Internet of Things" (IoT)?

Mitglieder des Informationsrechtsausschusses:

Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)
Rechtsanwältin Isabell Conrad, München
Rechtsanwalt Prof. Niko Härting, Berlin
Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
Rechtsanwalt Prof. Dr. Jochen Schneider, München (Berichterstatter)
Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
Rechtsanwalt und Notar Ulrich Volk, Wiesbaden
Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung:

Rechtsanwalt Thomas Marx

Verteiler Europa

Europäische Kommission

- Generaldirektion Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament

- Ausschuss Recht
- Ausschuss Industrie, Forschung, Energie
- Ausschuss Binnenmarkt und Verbraucherschutz
- Ausschuss für Wirtschaft und Währung

- Rat der Europäischen Union
- Ständige Vertretung der Bundesrepublik Deutschland bei der EU
- Justizreferenten der Landesvertretungen
- Der Europäische Datenschutzbeauftragte
- Rat der Europäischen Anwaltschaften (CCBE)
- Vertreter der Freien Berufe in Brüssel
- Bundesverband der Deutschen Industrie (BDI) in Brüssel
- Deutscher Industrie- und Handelskammertag (DIHK) in Brüssel

Verteiler Deutschland

- Bundesministerium des Innern
- Bundesministerium der Justiz

- Landesjustizverwaltungen

- Rechtsausschuss des Deutschen Bundestages
- SPD-Fraktion im Deutschen Bundestag
- CDU/CSU-Fraktion des Deutschen Bundestages, Arbeitsgruppe Recht
- Fraktionen BÜNDNIS 90/DIE GRÜNEN im Deutschen Bundestag
- FDP-Fraktion im Deutschen Bundestag
- Fraktion DIE LINKE im Deutschen Bundestag
- Die Datenschutzbeauftragten des Bundes und der Länder

- Vorstand und Geschäftsführung des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Vorsitzende des FORUMs Junge Anwaltschaft

- Deutscher Richterbund
- Bund Deutscher Verwaltungsrichter

- Deutscher Steuerberaterverband
- GRUR
- BITKOM
- DGRI
- Bundesverband der Freien Berufe

- Bundesrechtsanwaltskammer
- Bundesnotarkammer
- Deutscher Notarverein e. V.

- Redaktion NJW
- JUVE-Verlag
- ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene

---

A. Thesen

- Die Konsultation der Europäischen Kommission steht im Widerspruch zum gegebenen Rechtsrahmen für die Verarbeitung von Daten und dessen Prinzipien ebenso, wie sie die Entwicklung zur Datenschutz-Grundverordnung (DS-GVO) unberücksichtigt lässt.

- Die Antworten zu solchen Fragen sind für die rechtliche Einschätzung des Internet der Dinge (IoT) nicht zweckdienlich. Die Konsultation erfolgt losgelöst von dem zuvor von der Kommission vorgestellten Entwurf für eine DS-GVO, die gerade auf die Zukunftsfähigkeit des Datenschutzes abzielt, aber auch losgelöst von der Datenschutzrichtlinie 95/46/EG.

- Die *Einwilligung* ist nicht thematisiert. Die Zweck***bindung*** fehlt.

- Der Datenschutzrichtlinie und Entwurf der DS-GVO basieren auf dem **Verbotsprinzip**. Die Konsultation lässt das Verbotsprinzip hingegen außer Acht. Damit ist eine irritierende, die Antworten entwertende Verschiebung des Ausgangspunktes verbunden.

- Dass ***automatisierte Entscheidungen*** besonderer Beachtung bedürfen (Ansatz in Art. 15 Datenschutzrichtlinie 95/46/EG, etwas weiter § 6a BDSG), wird nicht ausreichend sichtbar. Die besondere Sensibilität des Themas heimlicher Bevorratung mit Daten wird für den Befragten nicht deutlich genug erkennbar und auch nicht im notwendigen Maße problematisiert. Die Notwendigkeit der Information an den Betroffenen wird nicht erwähnt (Art. 10, 11 DS-RL).

- **Durch das IoT werden praktisch alle Lebensäußerungen zu Daten, und zwar zu Daten „besonderen Datenkategorien“**. Bei ubiquitärer Datenverarbeitung bzw. bei Smartlife lassen sich gesundheitliche, politische, ethnische und Religions- bzw. Glaubenszugehörigkeit betreffende Daten nicht trennen bzw. nicht

vermeiden. Dies betrifft auch das Sexualleben. Die gesamte Intimsphäre muss zwangsläufig über die Kopplung diverser Daten, nicht zuletzt aus dem alltäglichen Leben i. V. m. der Steuerung des Hauses transparent werden. Es drohen massive Beeinträchtigungen von Grundrechten.

- Es besteht **Unverträglichkeit** der gesamten Konzeption der Befragung mit der bisherigen Rechtslage. Für die Zukunft des IoT müssten über das vorhandene Instrumentarium hinaus neben dem Instrument der Überwachungsgesamtrechnung (*Roßnagel*, NJW 2010, 1238) eine Methodik zu Ermittlung des Transparenzgrades und der „Belastung mit Daten für den Einzelnen geschaffen werden. Das IoT führt zur automatischen Komplettüberwachung und -datenbevorratung. Entsprechend komplett müsste die Ermittlung und Abdeckung der Gefährdungslagen für Gesellschaft und den Einzelnen erfolgen.

B. Stellungnahme

Fazit: Die Konsultation der Europäischen Kommission steht im Widerspruch zum gegebenen Rechtsrahmen für die Verarbeitung von Daten und dessen Prinzipien ebenso, wie sie die Entwicklung zur Datenschutz-Grundverordnung (DS-GVO) unberücksichtigt lässt. Aus Sicht des Deutschen Anwaltvereins sind die Antworten zu solchen Fragen für die rechtliche Einschätzung des Internet der Dinge (IoT) nicht zweckdienlich. Die Konsultation erfolgt losgelöst von dem zuvor von der Kommission vorgestellten Entwurf für eine DS-GVO, die gerade auf die Zukunftsfähigkeit des Datenschutzes abzielt, aber auch losgelöst von der Datenschutzrichtlinie 95/46/EG.

Auch der Entwurf der DS-GVO basiert – wie die Datenschutzrichtlinie – auf dem Verbotsprinzip. Die Konsultation lässt das Verbotsprinzip hingegen außer Acht. Damit ist eine irritierende, die Antworten entwertende Verschiebung der Prämissen verbunden.

Zu dem Entwurf der DS-GVO hat der Deutsche Anwaltverein (DAV) bereits Stellung genommen.[1]

[1] http://www.anwaltverein.de/downloads/Stellungnahmen-11/Stellungnahme-47.2012.pdf

Ausgangsfrage:

Die Kommission führt eine öffentliche Konsultation zum sog. **Internet der Dinge durch**, deren Ergebnisse in eine von der Europäischen Kommission bis Sommer 2013 angekündigte neue Empfehlung zu diesem Thema einfließen werden.

http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance:

Die Überschrift:

The Internet is gearing up for the next technological revolution: communication with and among objects. How would you envisage the "governance" of such an "Internet of Things" (IoT)?

I. Bewertung und Richtigstellung

1. Der Fragebogen und die Hintergrundinformationen sind von einer **einseitig** technologiefreundlichen Haltung ohne Referenz auf bestehendes Recht bestimmt, worauf (als bestehendes Datenschutzsystem) die Fragen aufbauen. Sowohl das bestehende Datenschutzrecht (Datenschutzrichtlinie 95/46/EG) mit voll harmonisierender Wirkung[2] als auch die im sich Gesetzgebungsverfahren befindliche DS-GVO werden nicht ausreichend dargestellt und gewürdigt, deren Grundprinzipien der Zulässigkeit entstellt. Soweit Referenzen gegeben werden, geschieht dies nur rudimentär, im Ergebnis sogar missverständlich, weil das Grundprinzip **nicht hinreichend vermittelt wird**.

2. Die Fragen setzen voraus, dass das Internet zu fördern ist („*zur Realisierung des enormen wirtschaftlichen und gesellschaftlichen Potentials des Internets der Dinge* ...."), ohne aber wesentliche Vorgaben des Datenschutzes de lege lata zu berücksichtigen. Die Fragen geben den Anschein, als ob Datenschutz erst erfunden, die Datenschutzrichtlinie 95/46/EG erst geschaffen und die DS-GVO nicht in Arbeit wäre (de lege ferenda). Die bereits bei e-mobility, smart grids u. ä.[3] erkannten Probleme sind nicht berücksichtigt, ebenso nicht die Maßgaben gegen *Totalerfassung*[4].

Die Entscheidungen des Bundesverfassungsgerichts (BVerfG) sind auch für die Kommission relevant, da Art. 8 Abs. 1 Grundrechte-Charta einen ganz ähnlichen Schutzbereich hat wie das deutsche Grundrecht auf informationelle Selbstbestimmung. Die Grundrechte-Charta hat

---

[2] EuGH v. 24.11.2011 - C-468/10 C-469/10.

[3] S. z.B. *Wiesemann*, MMR 2011, 213; s.a. working paper der Gruppe Art. 29: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf.

[4] S. z.B. BVerfG v. 2.3.2012 – 1 BvR 256/08 zur Vorratsdatenspeicherung. Zum Ansatz, der Totalerfassung sei zu begegnen, wenn auch vorliegend (GPS-sender am Auto) nicht gegeben s. BGH 24.01.2001, NJW 2001, 1658, BVerfG v. 12.04.2005, 2 BvR 581/01, CR 2005, 569 - Beweisgewinnung unter Verwendung von GPS.

gemäß Art. 6 Abs. 1 EUV den Rang von primärem Gemeinschaftsrecht. In der Praxis des EuGH wird Art. 8 Abs. 1 Grundrechte-Charta angewendet[5]. Als zentrales Recht des einzelnen muss dieses Recht auf informationelle Selbstbestimmung erhalten bleiben. Die gilt auch für das ergänzende *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*[6] Diesem Recht widersprechen die favorisierten „automatischen" Entscheidungs- und Verknüpfungsprozesse, wenn sie nicht vom Einzelnen gesteuert werden.

3. Die dritte Frage in Section 1 lautet: „***Traditional data protection principles include fair and lawful data processing; data collection for specified, explicit, and legitimate purposes; accurate and kept up-to-date data; data retention for no longer than necessary****. Do you believe that additional principles and requirements are necessary for IoT applications."* Eine Beantwortung dieser Frage zu Section 1 in Form der vorgegebenen Wahlmöglichkeiten impliziert praktisch, eine reine Technologiefreundlichkeit zu bejahen und den status quo mit der DS-RL und de lege ferenda mit der DS-GVO sowie der diesen zugrunde liegenden Prinzipien, etwa Art. 8 der Grundrechte-Charta zu negieren.

Dies gilt besonders für Ziffer 1., der für den DAV maßgeblichen Section „Privacy". Unter Section 1 „*Privacy*" wird im ersten Abschnitt/Feld die *Zweckentfremdung* der Daten als Scenario vorangestellt:

„*Bearing in mind that important benefits for society as a whole, such as in smart transportation systems, smart cities, pollution control, and sustainable consumption, are to be expected with IoT systems, it may be acceptable that data are used beyond the sole purpose of the application (e.g., for a service provider to run statistics on your smart meter usage)*."

Und sodann wird nach der Einstellung zur **Zweckentfremdung** gefragt, wie oben zitiert.

Diese Abfrage zur Zweckentfremdung konfligiert mit den maßgeblichen Ideen des Datenschutzes, zu denen allerdings in der dritten Frage zu Section 1 der Bezug hergestellt wird (Art. 6 Datenschutzrichtlinie 95/46/EG).

4. Dass ***automatisierte Entscheidungen*** besonderer Beachtung bedürfen (Ansatz in Art. 15 Datenschutzrichtlinie 95/46/EG, etwas weiter § 6a BDSG), wird nicht ausreichend sichtbar.

---

[55] Vgl. Urteil des EuGH v. 09.11.2010, verb. Rs. C-92/09 und C-93/09, Volker und Markus Schecke GbR, Hartmut Eilert gegen Land Hessen. Am 09.11.2010 hat der EuGH entschieden, dass die Veröffentlichung der Empfänger von Agrarbeihilfen in der bisherigen Form nicht mit dem Unionsrecht konform ist.

[6] BVerfG v. 27. 2. 2008 - 1 BvR 370/07 -, - 1 BvR 595/07

Die besondere Sensibilität des Themas heimlicher Bevorratung wird für den Befragten nicht deutlich genug erkennbar und auch nicht im notwendigen Maße problematisiert. Die Notwendigkeit der Information an den Betroffenen wird nicht erwähnt (Art. 10, 11 DS-RL).

In der Befragung wird nicht systematisch nach den ***Prinzipien*** gefragt, die der zu unterstellenden Bedrohungslage entsprächen, wenn automatisiert Entscheidungen ausgelöst, Querverbindungen profilabhängig hergestellt und global vermittelt würden, ggf. im Rahmen einer Gemengelage von personenbezogenem Content, personenbezogenen „smart-life"-, Nutzungs- und Bezahldaten. Solche Prinzipien wären etwa (Beispiele, nur als Illustration):

- Zweckbindung auf Basis Sphärenbildung mit strikter, einfacher Haftungsregelung bei Verletzung,

- Verbot der Profilbildung bzw. Nutzung zu anderen als dem ursprünglichen Zweck,

- Anonyme Bezahlung,

- Keine Kopplung von Content, Datenspuren der Nutzung und Bezahlung (einschl. smart e- ..., mobile ...),

- Strikte Zweckbindung für Clearingstellen, Clearingsysteme,

- Verfalldatum für Daten als Zahlungsmittel,

- Einwilligung in verschiedenen Formen, AGB-fest,

- (Gesamt-) Beaufschlagung fühl- und steuerbar machen gegenüber einer praktischen Total-Erfassung und Total-Biometrie.

5. Die dritte Frage zu Section 1 geht davon aus, dass traditionelle Datenschutzprinzipien bestimmte Maßgaben inkludieren, wie oben zitiert.

Das vorrangige *Verbotsprinzip* wird ebenso wenig wie die *Zulässigkeit*svoraussetzungen (Art. 7) **dargestellt**. Die im Fragebogen genannten Grundsätze sind **keine Zulässigkeitsvoraussetzungen**, sondern *Qualitätsgrundsätze*, Art. 6 (wenn denn die Datenverarbeitung erlaubt ist).

Die *Einwilligung* ist nicht thematisiert. Die Zweck***bindung*** fehlt. Es wird die Frage gestellt, ob *zusätzliche* Prinzipien speziell für die IoT-Applikationen erforderlich wären. Diese Art und Ebene der Frage klammert das Hauptprinzip, nämlich das Verbot, kombiniert mit Erforderlichkeit, was den wesentlichen wirtschaftlichen Bereich betrifft, aus. Die eigentlichen Zulässigkeitsvoraussetzungen werden nicht dargestellt.

6. Aufgrund des stark vereinfachten rechtlichen Bezugs wird mitunter der Anschein erweckt, die Konsultation gehe von einem nicht der Rechtslage entsprechendem Datenschutzverständnis aus und zwar sowohl de lege lata (Datenschutzrichtlinie 95/46/EG) als auch de lege ferenda (DS-GVO).

Eine pragmatische Herangehensweise bei der Beantwortung des Fragebogens erscheint nur dann möglich, wenn zumindest klargestellt wird, dass die Fragestellungen und v. a. die Hinweise dazu auch an dem Entwurf der DS-GVO zu orientieren sind. Ansonsten würde „IoT" vorangetrieben und entwickelt, ohne dass die Querverbindung zur DS-GVO bestehen würde.

Unter diesen Aspekten hält der DAV die Antworten auf den Fragebogen für nicht aussagekräftig bzw. beinhaltet der Fragebogen das Potential, datenschutzrechtlich in die Irre zu führen. Er widerspricht dem Vorhaben der Kommission mit der DS-GVO hinsichtlich der zentralen Frage der Voraussetzungen für Datenverarbeitung.

7. **Section 2** betrifft Safety and Security. Die Thematik ist wichtig, weil die „Sicherheit" Voraussetzung für eine Reihe von möglichen Problemlösungen ist, so insbesondere Anonymität, Abschottung (etwa völlige Trennung von Vergütungs- und Leistungsinformationen als konkrete Systeme) und Clearing Stellen.

Guidelines u. ä., also Standards, reichen als Instrument keinesfalls aus, so dass die Fragen in Section 2 zwar beantwortbar sind, **aber auf ein unzureichendes Ziel gerichtet wären**.

"Just as we need to protect against security attacks in the existing Internet, we should also consider information security and safety implications in the Internet of Things. Within the IoT autonomous objects may act on behalf of people and they will also need adequate protection against false requests for information and protection against unauthenticated commands.
At a minimum, the confidentiality, integrity and availability of IoT data and services must be safeguarded. User authentication, device and data authenticity, and data quality must be ensured. At the same time the data source has to be trusted, while unauthorised modifications of the data have to be prevented." (Einleitung Section 2 Absätze 1 und 2)

Das Einbauen der Privacy erfordert zunächst eine grundsätzliche konzeptionelle Gestaltung. Dies ist Grundvoraussetzung für Technikgestaltung. Schon die DS-GVO lehnt diese konzeptionelle Gestaltung ab, dort sind personenbezogene Daten das Schutzobjekt. Auch in der Konsultation fehlt der Gedanke der konzeptionellen Gestaltung. Damit fehlt auch eine persönlichkeitswahrende Ausrichtung, etwa Privacy Enhancing Technology (PET), Privacy by design u. ä. (wozu die DS-GVO Ansätze enthält). Genau zur Ausgestaltung dieser Prinzipien wäre aber zu befragen.

Die Frage ist zudem, ob bzw. wie es möglich ist, die einmal aus dem nationalen und dem EU-Kontrollbereich herausgelangten Daten überhaupt noch so zu beherrschen, dass die Grundprinzipien des „Datenschutzes“ (Privacy) und zudem Vertraulichkeit und Integrität eingehalten und kontrolliert werden könnten. Dass dies nicht der Fall ist, liegt auf der Hand. Die Kommission müsste in ihrer Konsultation also richtigerweise fragen, wie die entsprechenden Normen für Sicherheit, Abschottung u. ä. **international erreichbar und durchsetzbar** sind.

II. Inhaltliche Antwort, Vorschlag zur Ausgestaltung der weiteren Arbeit zu IoT

1. Die internationale Vernetzung erfordert ein international „kompatibles“ Schutzgut. Datenverkehrsregeln reichen nicht. Die Konsultation müsste zumindest die Grundprinzipien des Datenschutzes berücksichtigen und darauf aufbauen.

1.1 Die Tendenz „IoT“ führt unweigerlich zu noch stärkerer Vernetzung, Globalisierung und somit Allgegenwärtigkeit der Absonderung von Daten. Die Frage, welches **zusätzliche** Prinzip berücksichtigt werden müsste bzw. dazu geschaffen werden müsste, lässt sich naturgemäß nicht einfach beantworten. Der Umfang und der Grad an Bedrohungslagen wären jedenfalls nicht national und auch nicht nur EU-spezifisch definier- und regelbar. Als einschlägige Referenz wären in der Konsultation Art. 8 Grundrechte-Charta und Art. 7 Datenschutzrichtlinie 95/46/EG i. V. m. Art. 6 und 8 DS-RL zu nennen.

1.2 Als oberstes Prinzip müsste neben der **Ausbalancierung des Verbotsprinzips** durch weitere Maßgaben ein international durchsetzungsfähiges **Rechtsgut** bzw. Schutzgut stehen. Die Datenschutzrichtlinie und der Entwurf der DS-GVO verstärken die Fokussierung auf **Daten** und **verhindern** damit die Kompatibilität i. S. einer möglicherweise global geltenden Schutzidee des international vermittelbaren Schutzguts.

2. Die *Einwilligung* muss in ihrem Stellenwert völlig anders eingeordnet werden, als dies bisher vorgesehen ist. Die Einwilligung wird nach dem Entwurf der DS-GVO stark abgeschwächt werden, da bei einseitigen Machtverhältnissen die Einwilligung unwirksam wäre. Einseitige Machtverhältnisse wären, wenn sich jemand in das Internet der Dinge begibt, an der Tagesordnung. Das heißt, dass die Einwilligung nirgends gelten würde. Die Alternative wäre, dass es keine Monopolisten, keine Anbieter geben dürfte, die gegenüber dem Betroffenen ein „erhebliches Übergewicht" mit der Folge eines „erheblichen Ungleichgewichts" (Art. 7 Abs. 4 DS-GVO) darstellen würden.

3. Das **Hauptanliegen** dieser *Stellungnahme* zu der Konsultation ist, die parallel laufenden Planungen zur DS-GVO zu berücksichtigen. Bei der Auswertung des Konsultationsergebnisses gilt es, die Entwicklung im Bereich der DS-GVO zu berücksichtigen. Dabei muss auch im Blick behalten werden, dass die konkreten Fragen die Grundkonzeption des Datenschutzes nicht bzw. nur stark vereinfacht widergespiegelt haben. . Die entscheidende Frage ist: Ist das Internet der Dinge auf der Basis der Grundprinzipien, insbes. des Verbotsprinzips, das die Datenschutzrichtlinie 95/46/EG und die DS-GVO beherrscht, überhaupt realisierbar?

4. Berechtigung bestünde zu solchen Fragen, die die Datenschutzrichtlinie 95/46/EG und v. a. die DS-GVO ansprechen. Denn es ist sehr zweifelhaft, ob das EU-Datenschutzkonzept, insbesondere die DS-GVO, solchen technischen Entwicklungen, nach denen hier gefragt wird, standhalten würde bzw. ob das Konzept dafür nicht stark geändert und angepasst sein müsste.

5. Das im Rahmen der Umfrage dargestellte Datenschutzverständnis ist stark vereinfacht, sodass teilweise erhebliche **Lücken** entstehen, die beseitigt werden müssen.

Es sollte angegeben werden, welche Prinzipien in der DS-RL und der DS-GVO mit welchem Gewicht versehen auch das Thema IoT adäquat erfassen könnten.
Es muss also gefragt werden nach dem logischen Verhältnis von:

- Verbot,
- Vermeidung,
- Sparsamkeit,
- Erforderlichkeit,
- Zweckbindung.
- Transparenz und Accountability.

Die Konsultation zu IoT zielt auf **Vernachlässigung** der genannten Prinzipien. Gefragt wird nach zusätzlichen, anderen Prinzipien.

Die Antworten sind nicht rechtskonform verwertbar, wenn nicht eine **Kompensation** der aufgegebenen Prinzipien erfolgt. Danach müsste gefragt (und geforscht) werden.

6. Art. 5 der DS-GVO entspricht weitgehend der bisherigen Datenschutzrichtlinie 95/46/EG. Nach a) müssen personenbezogene Daten „*auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise*“ verarbeitet werden. Mit einer Mehrfachbeaufschlagung bzw. Cross-Informationssträngen mit teils automatisierten und teils „heimlich“ ausgeführten Entscheidungs- und Informationssträngen ist diese Regelung nicht vereinbar. Das in der Konsultation genannte Beispiel zum automatischen Verstellen des Weckers vermag das Problem nicht zu veranschaulichen. Anders gesagt: Das IoT ist mit Art. 5 a) DS-GVO in keiner Weise vereinbar. Die Rechtsmäßigkeit mag herstellbar sein. Es mag auch möglich sein, das IoT mit dem Grundsatz von Treu und Glauben vereinbar zu gestalten. In einer für die betroffene Person nachvollziehbaren Weise dürfte die Verarbeitung kaum möglich sein. Liest man die Konsultation, scheint das Gegenteil gewollt zu sein.

Noch gravierender ist der Widerspruch zu Art. 5 b) DS-GVO. Danach müssen die Daten für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiter verarbeitet werden. Während der zweite Halbsatz sich vielleicht steuern lässt, ist der erste Halbsatz nicht erfüllbar. Die Festlegung wäre noch denkbar. Es muss sich aber um eine genauere Festlegung handeln. Die Eindeutigkeit ist wohl kaum einhaltbar.

Die weiteren Anforderungen, die in Art. 5 DS-GVO gestellt werden, dürften ebenfalls im IoT kaum erfüllbar sein.

7. Nach Datenschutz-RL und ggf. Art. 6 DS-GVO gilt, wie erwähnt, das ***Verbotsprinzip***. Wie angedeutet, wäre die Rechtmäßigkeit herstellbar, aber an Bedingungen geknüpft. Die *Einwilligung*, die in 6 a) vorgesehen ist, mag einholbar sein. Auch hier aber müssen die Zwecke genau festgelegt werden. Es ist kaum vorstellbar, wie dies transparent geschehen soll, so dass die Zwecke bei einer integrierten Wirkung von Informationen festgelegt werden, wie in den diversen Beispielen auch für Smartlife beschrieben worden ist. Wichtig aber ist weiter, dass gemäß Art. 7. Abs. 4 DS-GVO die Einwilligung keine Rechtsgrundlage ist, wenn zwischen dem Betroffenen und dem für die Bearbeitung Verantwortlichen ein erhebliches

Ungleichgewicht besteht. D. h., dass die Einwilligung in noch wesentlich weniger Fällen wirksam gegeben werden kann, als nach der bisherigen Datenschutzrichtlinie. Das Instrument Einwilligung entfällt praktisch.

Art. 6 DS-GVO regelt in Abs. 1 b) das Erforderlichkeitsprinzip, d. h., es wird mit dem Verbotsprinzip in Art. 6 Abs. 1 Satz 1 gekoppelt. Die Erforderlichkeit ist praktisch unabdingbare Voraussetzung, soweit es um die Kategorie des Art. 6 Abs. 1 b) geht, um die Rechtmäßigkeit herzustellen bzw. eine Ausnahme vom Verbotsprinzip darzustellen. Auch die übrigen Varianten sind letzten Endes Umschreibungen bzw. dem Verbotsprinzip ähnliche Kategorien.

8. Durch das IoT werden praktisch alle Lebensäußerungen zu Daten und zwar zu „besonderen“: Verschärfte Regeln gelten für die *Verarbeitung besonderer Datenkategorien*. Diese sind in Art. 9 Abs. 1 DS-GVO aufgeführt. Über diesen Katalog lässt sich trefflich streiten. Dies soll hier nicht vertieft werden. Wichtig ist, dass die Verarbeitung personenbezogener Daten, die zu diesen Kategorien gehören, zunächst untersagt ist. D. h., dass hier ein weiteres Mal das Verbotsprinzip ausgesprochen wird und zwar sozusagen unter Aushebelung von Art. 6 DS-GVO. Die Rechtsmäßigkeit der Verarbeitung nach Art. 6 kann also nicht ohne weiteres für die besonderen Kategorien von personenbezogenen Daten hergestellt werden. Vielmehr muss dann nach Art. 6 Abs. 2 einer der dann aufgeführten Fälle vorliegen. Bei ubiquitärer Datenverarbeitung bzw. bei Smartlife lassen sich gesundheitliche, politische, ethnische und Religions- bzw. Glaubenszugehörigkeit betreffende Daten nicht trennen bzw. nicht vermeiden. Dies betrifft auch das Sexualleben. Die gesamte Intimsphäre muss zwangsläufig über die Kopplung diverser Daten, nicht zuletzt aus dem alltäglichen Leben i. V. m. der Steuerung des Hauses transparent werden.

Wie sich hier die Abgrenzung vollziehen soll, wird nicht deutlich. Die Stichworte dazu sind neben den Smartphones, Smart metering, v. a. Smart Home Networks und dabei etwa die Aufzeichnung von Schlafdaten. Ob und inwieweit es sich bei den zwangsläufig anfallenden Daten um Gesundheitsdaten – etwa bei den Schlafdaten – handelt, wird nicht leicht ersichtlich sein bzw. entschieden werden können. Da die Fehlbestände automatisch disponiert werden, sich dies auch auf Hygiene und evtl. auch auf pharmazeutische Kategorien beziehen mag, dürfte es nicht ausbleiben, dass laufend Gesundheitsdaten festgehalten werden und mithin die Entäußerung der Intimsphäre zwangsläufig ist. Dass dies nahezu zwangsläufig sein muss, wenn der Zahlungsverkehr noch gekoppelt ist, sei nur am Rande erwähnt.

9. Die Konzeption der Befragung macht die bestehende **Unverträglichkeit** der Thematik mit der bisherigen Rechtslage nicht deutlich. Für die Zukunft des IoT müssten über das vorhandene Instrumentarium hinaus neben dem Instrument der Überwachungsgesamtrechnung (*Roßnagel*, NJW 2010, 1238) eine Methodik zu Ermittlung des Transparenzgrades und der „Belastung mit Daten für den Einzelnen“ geschaffen werden. Das IoT führt zur automatischen Komplettüberwachung und -datenbevorratung. Entsprechend komplett müsste die Ermittlung und Abdeckung der Gefährdungslagen für Gesellschaft und den Einzelnen erfolgen.