scope & focus
Service-Gesellschaft mbH

Internet of Things (IoT) und Datenschutz – geht das?

Dipl.-Ök. Stephan Rehfeld

1

scope & focus
Service-Gesellschaft mbH

Was ist Datenschutz?

Erläuterung

- Das Recht auf informationelle Selbstbestimmung ist im Recht Deutschlands das Recht des Einzelnen, **grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen**. Es ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Datenschutz-**Grundrecht**, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird. […] Personenbezogene Daten sind jedoch nach Datenschutz-Grundverordnung und **nach** Art. 8 **der EU-Grundrechtecharta geschützt**.

Quelle: https://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung

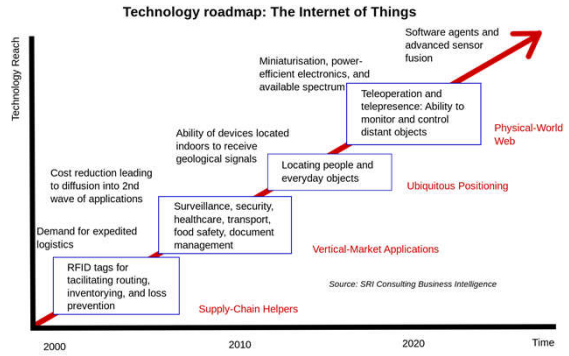
2

scope & focus Service-Gesellschaft mbH

Was ist das Internet of Things (IoT)

Definition

- Das Internet der Dinge ([…] Internet of Things, […] IoT) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.



Quelle: https://de.wikipedia.org/wiki/Internet_der_Dinge

3

scope & focus Service-Gesellschaft mbH

PRAXISBEISPIELE

4

scope & focus Service-Gesellschaft mbH

Beispiel: Fitnesstracker

Fitnesstracker: Strava-Aktivitätenkarte legt Militärbasen und Soldaten-Infos in aller Welt offen

Nicht nur Zivilisten, sondern auch Soldaten tracken offenbar fleißig ihre Bewegungen. Eine von Strava erstellte Weltkarte aller Aktivitäten legt deshalb teilweise geheime Militärbasen offen und zeigt beispielsweise regelmäßige Jogging-Routen.

Quelle: https://www.heise.de/newsticker/meldung/Fitnesstracker-Strava-Aktivitaetenkarte-legt-Militaerbasen-und-Soldaten-Infos-in-aller-Welt-offen-3952875.html

Wo die Bundeswehr joggen geht: Fitness-App entblößt Militärbasen in Konfliktgebieten

Fitbit sammelt Daten über Laufrouten auf der ganzen Welt und stellt sie ins Internet. Die Karte macht damit ungewollt geheime Camps und Bewegungsprofile in Kampfzonen sichtbar. Auch bei der Bundeswehr in Afghanistan wird fleißig trainiert.

Quelle: https://netzpolitik.org/2018/wo-die-bundeswehr-joggt-fitness-app-entbloesst-militaerbasen-in-konfliktgebieten/

5

scope & focus Service-Gesellschaft mbH

Beispiel: Staubsaugerroboter

Heinzelmänner

Saugroboter mit Raumerkennung und App-Steuerung

Auf Knopfdruck eine saubere Wohnung bis in den letzten Winkel – das versprechen moderne Saugroboter mit Kamera- oder gar Laser-Distanz-Navigation. Wir haben bei sechs Topmodellen getestet, wie gut sie saugen und ob sie auch beim Datenschutz sauber arbeiten.

Von Stefan Porteck

Abwaschen, staubsaugen, den Müll runterbringen, darauf hat doch niemand Lust. Also packt man das Geschirr in die Spülmaschine und drückt den Müll den Kindern aufs Auge. Bleibt nur das zeitraubende Staubsaugen. Das sollen nun Roboter genauso gut erledigen.

Quelle: https://www.heise.de/select/ct/2018/06/1521162153991864

25.07.2017 10:34 Uhr

Roomba: Hersteller der Staubsaugerroboter will Karten der Wohnungen verkaufen

Bislang sammeln die Roombas Daten über ihre Umgebung vor allem, um die besser reinigen zu können. Bald sollen die Daten der Staubsaugerroboter aber an Hersteller von Smart-Home-Geräten verkauft werden. Das soll die intelligenter machen.

Von Martin Holland

Quelle: https://www.heise.de/newsticker/meldung/Roomba-Hersteller-der-Staubsaugerroboter-will-Karten-der-Wohnungen-verkaufen-3782216.html

6

scope & focus Service-Gesellschaft mbH

Beispiel: Fernseher

Datenkrake im Smart-TV: Klage gegen Samsung

Stand: 13.09.2016 | drucken

Mit seinem Smart-TV greift Samsung ungefragt Daten von Nutzern ab. Deshalb klagen wir gegen die Samsung Electronics GmbH.

Das Wichtigste in Kürze

- **Samsung-Fernseher, die mit dem Internet verbunden sind, senden direkt nach dem Einschalten sensible Daten an den Hersteller, ohne dass der Nutzer informiert wird.**
- **Nach einer Abmahnung der Verbraucherzentrale NRW hat Samsung die Einstellung nicht geändert.**
- **Am 10. Juni hat das Landgericht Frankfurt/Main sein Urteil gesprochen.**

Mit der Musterklage vor dem Landgericht Frankfurt am Main gegen einen der Marktführer für TV-Geräte wollen wir nun erreichen, dass Daten erst nach entsprechender Information durch die Gerätehersteller und nach Einwilligung der Nutzer übertragen werden. Konkret geht es um das Samsung-Modell UE40H6270. Der erste Verhandlungstermin fand am 19. Mai 2016 statt. Das Urteil wurde am 10. Juni verkündet.

Datenschutzerklärung muss klarer werden

Nachbessern sollte Samsung auch bei der Verbraucherinformation zur Nutzung von Smart-Hub. Darunter werden Funktionen zusammengefasst, die via TV-Gerät zum Beispiel auch Zugang zu Nachrichten- und Spiele-Apps bieten. Zwar wird hier vor der ersten Aktivierung die Einwilligung zur Erhebung und Verwendung von Daten verlangt. Doch die Datenschutzbestimmungen erstrecken sich über 56 Bildschirmseiten und sind so unverständlich, lang und kompliziert, dass kein durchschnittlicher Fernsehnutzer die Folgen seiner Zustimmung durchblickt. Mit der Klage wollen wir mehr Transparenz und Verständlichkeit im Kleingedruckten erreichen.

Vom Gang vor Justitia hätten wir übrigens abgesehen, wenn Samsung bereit gewesen wäre, in der Grundeinstellung der Geräte eine anonyme Nutzung ohne Datenübertragung vorzusehen. Die Standardeinstellungen müssen immer die datenschutzfreundlichsten sein. Die technische Möglichkeit, die Datenübertragung nachträglich zu deaktivieren, genügt nicht.

Quelle: https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/fernsehen/datenkrake-im-smarttv-klage-gegen-samsung-12319 7

scope & focus Service-Gesellschaft mbH

Beispiel: Spielzeug

My Friend Cayla

Vernichten Sie diese Puppe

Seite 2/2: Smart Toys sind häufig schlecht gesichert

INHALT

Es ist jedenfalls nicht das erste Mal, dass Verbraucherschützer vernetztes Spielzeug kritisieren. 2015 etwa gewann Hello Barbie einen Big Brother Award. Der Negativpreis wird jährlich für Personen und Produkte verliehen, die gegen den Datenschutz verstoßen oder rücksichtslos Daten sammeln. Im Fall der Barbie-Puppe kritisierten die Datenschützer, dass alle Sprachaufnahmen an die Server eines Unternehmens weitergeleitet wurden. Der Sicherheitsforscher Linus Neumann sagte, Kinder würden somit schon von klein auf mit der Abschöpfung von Daten konfrontiert.

Ebenfalls vor zwei Jahren sind Hacker in die Server des asiatischen Unternehmens VTech eingedrungen, das vernetztes Spielzeug und Lerncomputer herstellt. Dort fanden sie persönliche Daten von Kindern und Eltern sowie 190 Gigabyte Fotos und gespeicherte Chats. Die Hacker veröffentlichten die abgeschöpften Daten nicht. Der Angriff sollte bloß als Warnung dienen.

Die Hersteller haben andere Prioritäten

Der Fall von VTech hatte einmal mehr gezeigt, dass Hersteller smarter Geräte offenbar nicht oder nur schlecht die Daten ihrer Nutzer schützen. In der Branche des Internet der Dinge (IoT) gibt es regelmäßig Berichte über schlecht gesicherte Kameras und Haushaltsgeräte. Die Hersteller haben häufig andere Prioritäten als IT-Sicherheit oder Verschlüsselung, zudem fehlt es an Standards und Richtlinien, die es einzuhalten gilt.

Quelle: https://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur/seite-2 8

scope & focus Service-Gesellschaft mbH

Achtung TKG und StGB

Hersteller:

Nach § 90 Telekommunikationsgesetz (TKG) ist es verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen.

Betreiber:

§ 201 StGB - Verletzung der Vertraulichkeit des Wortes

§201a StGB - Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

9

scope & focus Service-Gesellschaft mbH

Beispiel: Sprachassistenten

UPDATE 20.12.2018 07:00 Uhr | c't Magazin

Amazon gibt intime Alexa-Sprachdateien preis

Durch einen Fehler von Amazon.de fielen rund 1700 Alexa-Sprachaufzeichnungen in die Hände eines Unbefugten.

Von Holger Bleich 1351

Ein Amazon.de-Kunde hatte die deutsche Niederlassung des Konzerns um Auskunft der zu ihm gespeicherten Daten nach DSGVO gebeten. Amazon stellte ihm zwei Monate später ein ZIP-Archiv bereit. Rund 50 der darin enthaltenen Dateien enthielten auf seine Person bezogene Daten. Allerdings fand er auch rund 1700 WAV-Dateien sowie eine PDF-Datei vor, die offensichtlich chronologisch unsortierte Transskripte darüber enthielt, was Amazons Sprachassistent Alexa aus Spracheingaben verstanden hat.

Intimsphäre verletzt

Die Sprachaufzeichnungen stammen hörbar aus der Intimsphäre fremder Personen, beispielsweise aus Wohnzimmer, Schlafzimmer und Bad. Anhand des Inhalts der Aufzeichnungen, etwa der Nennung von Namen und Abfragen lokaler Wettervorhersagen, konnte c't den Echo-Besitzer identifizieren. Dieser fiel aus allen Wolken, denn Amazon hatte ihn nicht über das Datenleck informiert, obwohl man dort bereits davon wusste.

Quelle: https://www.heise.de/meldung/Amazon-gibt-intime-Sprachdateien-preis-4254716.html

10

scope & focus
Service-Gesellschaft mbH

DATENSCHUTZANFORDERUNGEN

11

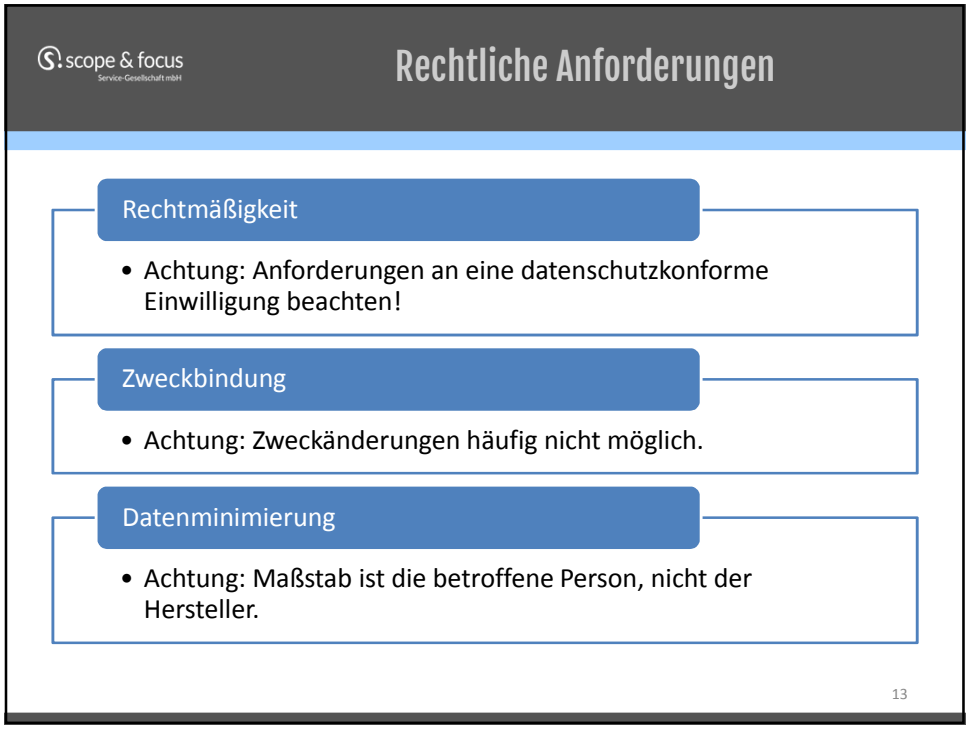
scope & focus
Service-Gesellschaft mbH

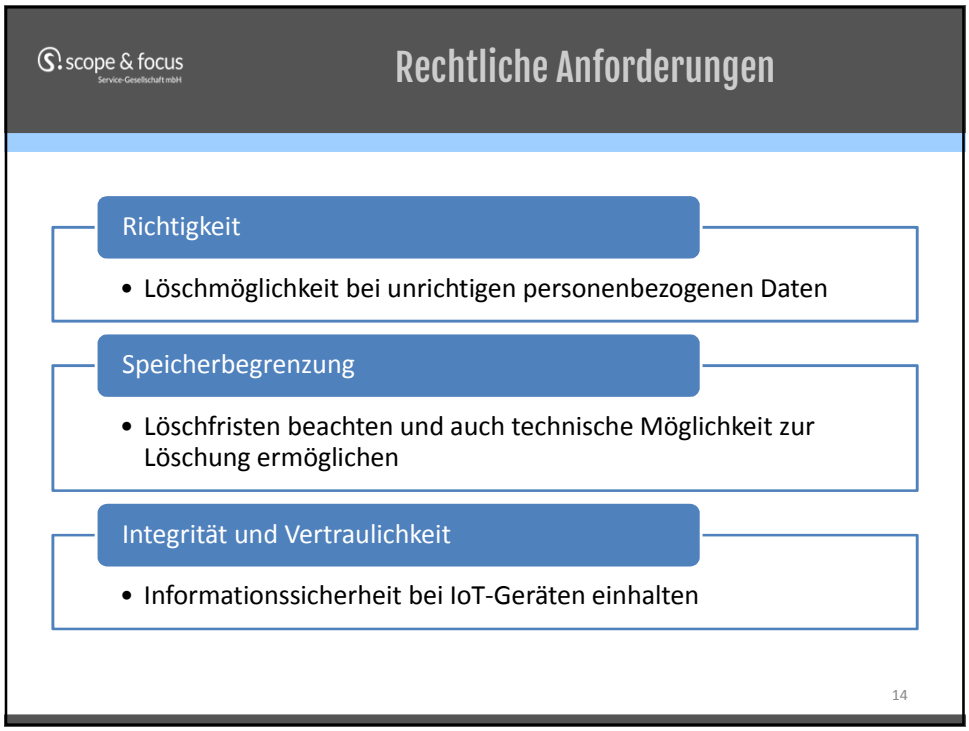
Kritik aus Sicht der betroffenen Personen

- Mangelnde Kontrolle der betroffenen Person über IoT-Geräte
- Informations-Asymmetrie
- Schlechte Implementierung der Einholung der Einwilligung
- Häufig keine oder wenige Informationen zu Zweckänderungen
- Keine Informationen über Datenauswertungen
- Keine oder schlechte Informationen über Profilbildungen
- Kaum Möglichkeiten der anonymen Nutzung von Diensten und Services
- Sicherheitsrisiken: Sicherheit vs. Effizienz

Literaturhinweis: Artikel 29-Gruppe, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 2014

12


scope & focus
Service-Gesellschaft mbH
Rechtliche Anforderungen
Rechtmäßigkeit
• Achtung: Anforderungen an eine datenschutzkonforme Einwilligung beachten!
Zweckbindung
• Achtung: Zweckänderungen häufig nicht möglich.
Datenminimierung
• Achtung: Maßstab ist die betroffene Person, nicht der Hersteller.
13


scope & focus
Service-Gesellschaft mbH
Rechtliche Anforderungen
Richtigkeit
• Löschmöglichkeit bei unrichtigen personenbezogenen Daten
Speicherbegrenzung
• Löschfristen beachten und auch technische Möglichkeit zur Löschung ermöglichen
Integrität und Vertraulichkeit
• Informationssicherheit bei IoT-Geräten einhalten
14

Betroffenenrechte

Betroffenenrechte

- Auskunft
- Berichtigung
- Einschränkung
- Löschung
- Datenportabilität

Hinweispflichten

- Artt. 13 und 14 DSGVO beachten

15

Privacy by Design und Privacy by Default

Privacy by Design

- Proaktiv nicht reaktiv; präventiv nicht „heilend“
- Datenschutz als Standard
- Datenschutz im Design integriert
- Keine Einschränkung der Funktionalität durch Datenschutz
- End-to-End-Sicherheit - Lebenszyklus-Schutz
- Sichtbarkeit und Transparenz
- Respekt vor der Privatsphäre der Benutzer

Privacy by Default

- Einstellungen so treffen, dass sie datensparsam sind

Literaturhinweis: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

16

scope & focus
Service-Gesellschaft mbH

Rechenschaftspflicht

Rechenschaftspflichten

- Meldung von Datenpannen
- Aufzeichnungen

17

scope & focus
Service-Gesellschaft mbH

scope & focus

Ihre Daten - mit Sicherheit!

Leonhardtstr. 2
30175 Hannover
T: 0511 | 364 221-0
F: 0511 | 364 221-99

Hoerneckestr. 19-21
28217 Bremen
T: 0421 | 369 3530-0
F: 0421 | 369 3530-99

www.scope-and-focus.com
information@scope-and-focus.com

Dipl.-Ök. Stephan Rehfeld
Dipl.-Wirt.-Ing. Ulrike Hauser

18