

## **Vierter Verbraucherdialog „Smart Home“ - Chancen nutzen, Risiken minimieren -**

### **Empfehlungen zum Verbraucher- und Datenschutz bei Smart Home-Angeboten für Anbieter sowie Verbraucherinnen und Verbraucher**

Mainz, 11.02.2016

*Die vorliegenden Empfehlungen zu „Smart Home“ beziehen sich vorzugsweise auf Nachrüstlösungen für den privaten Gebrauch. Sie sollen einerseits Anbietern Kriterien zur verbraucher- und datenschutzfreundlichen Angebotsgestaltung an die Hand geben sowie andererseits Verbraucherinnen und Verbrauchern Information und Hilfestellung bieten, worauf bei der Auswahl und Nutzung von Angeboten der intelligenten Heimvernetzung und -automation zu achten ist.*

*Die Empfehlungen wurden im vierten rheinland-pfälzischen Verbraucherdialog „Smart Home“ von Expertinnen und Experten des Verbraucher- und Datenschutzes, der Wirtschaft und Wissenschaft erarbeitet und verstehen sich als konstruktiver Beitrag für einen vorsorgenden, praxisnahen Verbraucher- und Datenschutz an einem noch jungen Markt.*

#### **I. Vorbemerkung**

Derzeit entsteht in Deutschland ein Volumenmarkt für nachrüstbare Lösungen. „Smart Home“ ist zunehmend im Handel präsent. Marktbeobachter gehen davon aus, dass kurz- bis mittelfristig ein starkes Wachstum für den Smart Home-Markt zu erwarten ist.

Damit hält die Digitalisierung weiter Einzug in die Wohn- und Lebensräume der Verbraucherinnen und Verbraucher. Das Internet der Dinge erreicht den Verbraucheralltag. Dies kann Chancen, aber auch Risiken bergen. „Smart Home“ kann zum Beispiel Sicherheit und Komfort im Alltag u.a. für ältere Menschen bringen. Gleichzeitig begegnet „Smart Home“ Bedenken und Unsicherheiten zum Beispiel bezüglich des Datenschutzes, hoher Kosten oder der technischen Installation und Anwendung.

Angesichts der permanenten technologischen Innovation und veränderter, komplexer Angebote stehen Verbraucherinnen und Verbraucher generell vor der Herausforderung, mit der rasanten Entwicklung am globalen Markt Schritt zu halten. Dabei sind das Kenntnisniveau und die Fertigkeiten im Umgang mit digitalen Angeboten unter Verbraucherinnen und Verbrauchern jeweils unterschiedlich ausgeprägt.

Smart Home-Angebote sollten daher grundsätzlich so ausgestaltet sein, dass auch Verbraucherinnen und Verbraucher ohne besondere Vorkenntnisse in der Lage sind, geeignete Angebote individuell auszuwählen und sicher und kompetent zu nutzen.

Von zentraler Bedeutung ist, dass Verbraucherinnen und Verbraucher sich auf eine sichere und datenschutzfreundliche Angebotsgestaltung mit fairen Vertragsbestimmungen und Erläuterungen verlassen können. Zudem bedarf es einer bedürfnisorientierten Dienst- und Produktentwicklung, Bedienfreundlichkeit und Transparenz. Für die Auswahl, Einrichtung und den Betrieb wesentliche Informationen sollten gezielt, verständlich und leicht auffindbar zur Verfügung stehen, damit Verbraucherinnen und Verbraucher informierte Entscheidungen treffen können.

Anbieter, die über das gesetzlich geforderte Maß hinaus Schutz- und Unterstützungsmaßnahmen vorsehen, tragen dazu bei, dass Verbraucherinnen und Verbraucher von Anfang an Vertrauen in neue Angebote haben und Mehrwerte erschließen können. Ein hohes Verbraucher- und Datenschutzniveau kann daher als Qualitäts- und Wettbewerbskriterium zugleich gelten, insbesondere vor dem Hintergrund eines globalen Marktes.

Verbraucher- und Datenschutz gelingt grundsätzlich nicht allein durch Regulierung, sondern auch durch verantwortungsbewusste Angebotsgestaltung, Transparenz und Information.

## **II. Vierter Verbraucherdialog „Smart Home“**

Der Verbraucherdialog ist ein Veranstaltungsformat des Ministeriums der Justiz und für Verbraucherschutz Rheinland-Pfalz in bewährter Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e.V. und dem rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Der vierte Verbraucherdialog fand von Juni 2015 bis Januar 2016 zum Thema „Smart Home“ in Mainz statt.

Das Format „Verbraucherdialog“ dient dem konstruktiven Austausch insbesondere mit Expertinnen und Experten aus Wirtschaft und Wissenschaft im Interesse eines vorsorgenden Verbraucher- und Datenschutzes. Er ist vorbereitend für gegebenenfalls politische Initiativen und staatliche Maßnahmen zur Verbraucheraufklärung und -information.

Nachfolgend genannte Verbände, Unternehmen, Behörden und Organisationen haben am vierten Verbraucherdialog „Smart Home“ teilgenommen. Die genannten Verbände, Unternehmen, Behörden und Organisationen haben an der Erarbeitung des vorliegenden Papiers mitgewirkt und unterstützen die Umsetzung und Verbreitung der gemeinsamen Empfehlungen gemäß der ihnen zur Verfügung stehenden Möglichkeiten.

## Teilnehmer am vierten Verbraucherdialog „Smart Home“:

- BHE Bundesverband Sicherheitstechnik e.V.
- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
- ChaosComputerClub
- digitalSTROM AG
- diхва GmbH
- eQ-3 AG
- Fachverband Elektro- und Informationstechnik Hessen/Rheinland-Pfalz (FEHR)
- Fraunhofer-Institut für Experimentelles Software Engineering (IESE)
- Landeszentrale für Medien und Kommunikation Rheinland-Pfalz
- Ministerium für Soziales, Arbeit, Gesundheit und Demografie Rheinland-Pfalz
- Projekt "Silver Tipps" der Johannes Gutenberg-Universität Mainz
- VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

### **III. Definition „Smart Home“**

Im vierten Verbraucherdialog wurde folgende Definition von „Smart Home“ zugrunde gelegt:

*Unter „Smart Home“ werden technische Verfahren, Systeme und Dienste in Wohnräumen, -häusern und der Wohnumgebung verstanden, die auf vernetzten Geräten und Installationen sowie automatisierbaren Abläufen basieren und zur Erhöhung der Wohn- und Lebensqualität, der Sicherheit sowie zur Steuerung der Energienutzung beitragen sollen. Hierunter fallen derzeit die Vernetzung von Haus- und Sicherheitstechnik, von Haushaltsgeräten und von Komponenten der Unterhaltungselektronik.*

*Kennzeichnend für „Smart Home“ sind u.a. die Kommunikation der Geräte untereinander sowie die Kommunikation der Geräte mit Anwendern und gegebenenfalls weiteren beteiligten Stellen. Die Geräte reagieren auf Datenübertragungen hausinterner und -externer Art sowie auf lokale Sensoren. Sie besitzen Schnittstellen, die über verschiedene Technologien, zum Beispiel über Internet und spezielle Apps, angesprochen werden können.*

Technische Verfahren, Systeme und Dienste, die gezielt der medizinischen Unterstützung und Notfallversorgung von älteren Menschen oder Menschen mit Behinderungen dienen, sind gesondert zu betrachten. Altersgerechte Assistenzsysteme für ein selbstbestimmtes Leben (Ambient Assisted Living) waren nicht explizit Gegenstand des vierten Verbraucherdialogs.

#### **IV. Gegenstand der Empfehlungen**

Die Empfehlungen beziehen sich vorzugsweise auf nachrüstbare Smart Home-Angebote, die individuell eingerichtet werden können oder durch eine kundige Fachkraft zu installieren sind. Die Empfehlungen umfassen grundsätzlich alle Lösungsmodelle, Kommunikationstechnologien und Anwendungsbreiten, die derzeit am deutschen Markt angeboten werden. Teils werden Konkretisierungen vorgenommen.

Smart Home-Angebote können realisiert werden als

- proprietäre Lösungen, die ausschließlich anbiereigene Komponenten einsetzen
- Lösungen, die eigene Komponenten und Komponenten ausgewählter Partner integrieren
- Systeme, die für beliebige Produkte grundsätzlich offen sind.  
Offene Lösungen basieren auf offenen Schnittstellen, wobei es verschiedene Standards gibt, die nicht zwingend miteinander interoperabel sind.

Die Kommunikation zwischen den Komponenten erfolgt funkbasiert oder auch leitungsgebunden. Die Anwendungsbreite reicht von speziell bis universell einsetzbaren Lösungen.

#### **V. Zielsetzungen und Schwerpunkte der Empfehlungen**

Die Empfehlungen für Anbieter zielen auf die praktische Umsetzung zusätzlicher beziehungsweise optionaler Vorkehrungen im Interesse eines vorsorgenden Verbraucher- und Datenschutzes. Sie betreffen insbesondere sicherheits-, anwendungs-, kosten- und datenschutzrelevante Kriterien unter Berücksichtigung technisch-organisatorischer Maßnahmen, vertragsrechtlicher Bestimmungen sowie Maßnahmen zur Verbraucherinformation.

Die Empfehlungen für Verbraucherinnen und Verbraucher wurden auf Grundlage der Empfehlungen für Anbieter entwickelt. Sie sollen zum Verständnis von Smart Home-Technologien beitragen, Verbraucherinnen und Verbraucher für mögliche Vorteile und Risiken sensibilisieren sowie auf eine informierte Kaufentscheidung und kompetente Nutzung von Smart Home-Angeboten hinwirken.

Die Empfehlungen gliedern sich in zwölf Schwerpunkte:

1. *Installation und Inbetriebnahme*
2. *Geräteeigenschaften*
3. *Bedienung*
4. *Kosten und Vertragsmodelle*
5. *Interoperabilität und Erweiterbarkeit*
6. *Haltbarkeit*
7. *Personenbezug und grundsätzliche Zweckbindung von Daten*
8. *Transparenz der Datenverwendung*
9. *Datensouveränität*
10. *Datensparsamkeit*
11. *Kontroll- und Steuerungsmöglichkeiten*
12. *Sicherheit bei Datenspeicherung, -übertragung und -zugriff*

Aus Verbraucherschutzsicht ist vor allem wichtig, dass die Einrichtung und Bedienung von Geräten und Diensten keine besonderen technischen Kenntnisse verlangt, dass Kosten und Vertragsbedingungen transparent dargestellt werden und dass Systeme über lange Zeiträume hinweg erweitert und in Stand gehalten werden können.

Aus Sicht des Datenschutzes muss beim Einsatz von Smart Home-Lösungen für die Verbraucherinnen und Verbraucher erkennbar sein, welche Daten, in welchem Umfang, in welcher Weise und zu welchem Zweck verarbeitet werden und welche Stellen auf diese zugreifen können. Zur Wahrnehmung ihrer Rechte müssen die Nutzerinnen und Nutzer über ausreichende Kontroll- und Steuerungsmöglichkeiten verfügen. Grundsätzlich sollten Smart Home-Lösungen eine pseudonyme beziehungsweise anonyme Verarbeitung vorsehen und personenbezogene Datenverarbeitungen im Wege von den Nutzerinnen und Nutzern aktiv zu wählender Optionen anbieten.

## **VI. Rechtsrahmen**

Die Empfehlungen setzen die Einhaltung und Anwendung der geltenden Rechtsvorschriften voraus.

Wichtige Rechtsgrundlagen sind zum Beispiel die Regelungen aus dem Bürgerlichen Gesetzbuch und dem Bundesdatenschutzgesetz. Zudem sind spezialgesetzliche Rechtsgrundlagen in den Blick zu nehmen. Hierzu gehören insbesondere das Telemedien- und Telekommunikationsgesetz sowie das Energiewirtschaftsgesetz.

Darüber hinaus gelten gesetzliche Vorschriften zur Einhaltung und Kennzeichnung technischer Sicherheitsnormen.

Daneben können freiwillige Zertifizierungsmöglichkeiten beispielsweise nach ISO 2700x herangezogen werden.

## **Empfehlungen für Anbieter zur verbraucher- und datenschutzfreundlichen Ausgestaltung von Smart Home-Angeboten**

### **1. Installation und Inbetriebnahme**

Smart Home-Geräte und -Dienste, deren Installation nicht bereits gesetzlich durch die kundige Fachkraft durchzuführen ist, sollten so gestaltet sein, dass ihre Installation und Inbetriebnahme nicht mehr als grundlegende technische Kenntnisse erfordern. Die verfügbaren Installationsanleitungen sollten allgemein verständlich sein und den Produkten in gedruckter Form beigelegt werden. Sie sollten sich auf die dem Nutzer gelieferte aktuelle Revision beziehungsweise Version eines Produktes beziehen. Im Falle eines Updates sollten gegebenenfalls angepasste Anleitungen kostenfrei zum Download zur Verfügung gestellt werden.

Nutzerinnen und Nutzer sollten bei der Ersteinrichtung angehalten werden, voreingestellte Passwörter zu ändern. Außerdem sollten Hinweise zu sicheren Passwörtern gegeben werden. Wünschenswert sind Mindestanforderungen an das Passwort (Zeichenanzahl, Groß-/Kleinschreibung, Ziffern, Sonderzeichen), deren Einhaltung beispielsweise durch die Abbildung einer „Ampel“ visualisiert wird.

Personenbezogene Daten wie zum Beispiel Name und Standort sollten nur abgefragt werden, soweit dies für die Nutzung erforderlich ist. Eine anonyme Einrichtung der verbundenen Geräte und Dienste sollte grundsätzlich möglich sein.

### **2. Geräteeigenschaften**

Wenn eine Funkreichweite angegeben wird, sollte sich bereits aus der Werbung mit technischen Daten ergeben, dass die tatsächliche Reichweite durch bauliche und andere Gegebenheiten deutlich davon abweichen kann. Die einzelnen Komponenten von Smart Home-Installationen sollten sich nach Möglichkeit im Sinne von „Plug & Play“ für den Nutzer auf einfache Weise weitgehend selbstständig miteinander verbinden. Dabei müssen Datenschutz und Sicherheit gewahrt werden.

Die Geräte sollten einen möglichst geringen Stromverbrauch aufweisen, insbesondere im Bereitschaftszustand. Bei batteriebetriebenen Geräten sollten Nutzerinnen und Nutzer vor dem Kauf auf den Batterietyp, die Lebensdauer der Batterie und mögliche Folgekosten hingewiesen werden.

Eine Fernwartung durch Service-Techniker sollte nur unter Einhaltung strenger Zugriffskriterien und nach technischer Freigabe durch den Nutzer im Einzelfall möglich sein. Das gilt insbesondere bei Nutzung von Geräten und Diensten über Clouds.

### **3. Bedienung**

Die Bedienung von Geräten und Diensten sollte möglichst einfach und intuitiv ausgestaltet sein. Bedienungsanleitungen sollten allgemein verständlich sein und alle wesentlichen Funktionen darstellen. Nutzerinnen und Nutzer sollten gegebenenfalls die Möglichkeit haben, verschiedene Benutzerkonten mit unterschiedlichen Berechtigungen einzurichten.

Nutzerinnen und Nutzer sollten technische Unterstützung auf unkomplizierte Weise erhalten können, zum Beispiel telefonisch, persönlich, per E-Mail, per Web-Chat, Fernwartung und in Form von Hilfetexten (sog. FAQs) im Internet. Die Unterstützung sollte vom Vertragspartner des Nutzers geleistet werden. Zusätzlich ist die Möglichkeit eines Kontakts zum Hersteller wünschenswert.

Die technische Unterstützung sollte für Nutzerinnen und Nutzer kostenlos oder nur mit geringen Entgelten verbunden sein. Die Kostensätze für die Einsätze von Service-Technikern bei den Nutzerinnen und Nutzern vor Ort sollten sich an der branchenüblichen Vergütung orientieren.

Die Bedürfnisse von älteren oder behinderten Menschen sollten grundsätzlich berücksichtigt werden. Nach Möglichkeit sollten Geräte und Dienste barrierefrei ausgestaltet werden. Dasselbe gilt für Möglichkeiten, technische Unterstützung zu erhalten.

Nutzerinnen und Nutzer treffen bei der Bedienung allgemeine Sorgfaltspflichten. Darüber hinaus sollte ihnen nicht mehr als die Pflicht zur Pflege und Absicherung eines Benutzerkontos und zur Durchführung von Updates auferlegt werden. Über das Vorhandensein von Updates sollte informiert werden, außerdem sollte nach Möglichkeit eine Option zur Wiederherstellung des vorherigen Zustands vorhanden sein. Nutzerinnen und Nutzer sollten über den Umfang ihrer Sorgfaltspflichten ausdrücklich informiert werden, d.h. nicht nur im Rahmen von Nutzungsbedingungen.

Geräte und Dienste müssen einen plötzlichen oder geplanten Stromausfall unbeschadet überstehen können. Nach dem Ausfall sollten alle Funktionen ohne Eingriff der Nutzerinnen und Nutzer wieder uneingeschränkt zur Verfügung stehen.

### **4. Kosten und Vertragsmodelle**

Durch Kauf von Geräten sollten Nutzerinnen und Nutzer das Recht erhalten, die darauf befindliche Software kostenfrei zu verwenden. Weiterhin sollten die Software-Updates zur Fehlerbehebung und Sicherheit für Nutzerinnen und Nutzer stets kostenfrei erhältlich sein. Auch die Nutzung von Clouds oder sonstigen internetbasierten Diensten sollte ohne weitere Kosten möglich sein, wenn die Grundfunktionen nur mittels Anbindung an das Internet verfügbar sind.

Verträge über die Nutzung von kostenpflichtigen Zusatzdiensten sollten erst dann zustande kommen, wenn der Nutzer ausdrücklich darin einwilligt. Die Dienste sollten über kurze Mindestvertragslaufzeiten verfügen.

Im Falle von Mietmodellen für die Gerätenutzung sollten Nutzerinnen und Nutzer stets die Möglichkeit erhalten, die Geräte zu kaufen.

Informationen zu Entgelten und Vertragsbedingungen sollten vollständig und in übersichtlicher Weise auf der Homepage der Anbieter abrufbar sein. Nutzerinnen und Nutzer sollten nicht mit versteckten Kosten belegt werden.

## **5. Interoperabilität und Erweiterbarkeit**

Geräte und Dienste sollten auf der Grundlage von offenen oder mit einer Vielzahl von Anbietern gemeinsam entwickelten Standards und Schnittstellen miteinander kommunizieren, soweit dies die Sicherheit nicht beeinträchtigt.

Installierte Systeme sollten mit neuen Geräten möglichst auch anderer Hersteller erweitert werden können. Nutzerinnen und Nutzer sollten die Möglichkeit erhalten, leicht an Informationen zu den untereinander interoperablen Geräten zu gelangen. Hersteller von Geräten sollten bei Angaben zur Kompatibilität von Standards und der Interoperabilität mit Geräten anderer Hersteller realistische Aussagen treffen.

Wenn für die Verwaltung oder Bedienung von Geräten und Diensten ein Fernzugriff durch den Nutzer vorgesehen ist, sollte dieser über alle verbreiteten Betriebssysteme für mobile Endgeräte per App und mittels Browserprogramm möglich sein.

Rückwärts- und Vorwärtskompatibilität sollten über lange Zeit bei Geräten und Diensten gewährleistet werden, soweit dies wirtschaftlich vertretbar ist.

Für Geräte und Dienste sollten lange Nutzungszeiträume vorgesehen werden, in denen installierte Systeme erweitert werden können.

## **6. Haltbarkeit**

Anbieter sollten Geräte und Dienste über eine möglichst lange Zeit hinweg unterstützen. Dazu gehören insbesondere technische Hilfe und die Bereitstellung von Sicherheitsupdates.

Ersatzteile sollten über eine möglichst lange Zeit bereitgehalten werden.

## **7. Personenbezug und grundsätzliche Zweckbindung von Daten**

Anbieter und Hersteller von Smart Home-Lösungen haben zu berücksichtigen, dass es sich bei den anfallenden Daten in der Regel um personenbezogene, jedenfalls personenbeziehbare Daten im Sinne von § 3 Abs. 1 BDSG handelt. Soweit bei rein technischen Daten (z.B. Sensorwerte) durch Verknüpfung mit weiteren Informationen ein Bezug zum jeweiligen Nutzer beziehungsweise Vertragspartner hergestellt werden kann, ergibt sich auch hier ein Personenbezug. Dieser Personenbezug besteht dabei unabhängig von der gegebenenfalls unterschiedlichen Sensitivität einzelner Datenkategorien.

Die Verwendung personenbezogener Daten ist nur zulässig, soweit dies eine Rechtsvorschrift erlaubt oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt).



Eine Einwilligung ist dabei an den Vorgaben des § 4a BDSG zu messen, d.h. sie muss insbesondere freiwillig und informiert erfolgen.

Als gesetzliche Erlaubnisvorschrift kommt insbesondere § 28 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Die Rechtsvorschriften adressieren stets die verantwortliche Stelle nach § 3 Abs. 7 BDSG. Neben den Nutzerinnen und Nutzern können dies zum Beispiel Anbieter, Hersteller, aber auch weitere eingebundene Dienstleister sein.

Dem Grundsatz der Zweckbindung entsprechend dürfen personenbezogene Daten nur zu dem Zweck verwendet werden, zu dem sie ursprünglich erhoben wurden. Eine darüber hinaus gehende zweckändernde Verwendung personenbezogener Daten, zum Beispiel zu Marketingzwecken, bedarf daher einer gesonderten datenschutzrechtlichen Rechtfertigung. Dies wird in der Regel nur im Wege der Einwilligung gemäß § 4a BDSG möglich sein.

## **8. Transparenz der Datenverwendung**

Zum effektiven Schutz des informationellen Selbstbestimmungsrechts von Nutzerinnen und Nutzern haben Hersteller und Anbieter von Smart Home-Anwendungen sicherzustellen, dass die stattfindenden Datenflüsse transparent und nachvollziehbar sind. Nur so werden die Betroffenen in die Lage versetzt, eine verantwortliche Entscheidung über die Nutzung einzelner Anwendungen zu treffen.

Der Grundsatz der Transparenz erfordert daher, dass Nutzerinnen und Nutzer vor der ersten Datenerhebung in leicht verständlicher und aussagekräftiger Form insbesondere Informationen zu den folgenden Punkten erhalten:

- Welche Daten auf welcher Rechtsgrundlage, in welchem Umfang, in welcher Weise und zu welchem Zweck verarbeitet werden. Hierzu gehört auch, welche Daten zur Erfüllung des Vertragszwecks erforderlich sind und welche gegebenenfalls zu anderen Zwecken erhoben werden.
- Wer für einzelne Datenverarbeitungsprozesse verantwortlich ist. Das gilt insbesondere auch bei der Einbindung Dritter. Soweit Dienstleister einbezogen werden, die für die Erfüllung des Vertragszweckes von wesentlicher Bedeutung sind, sollten die Nutzerinnen und Nutzer darüber informiert werden.
- Ob und in welchem Umfang Nutzerinnen und Nutzer die Möglichkeit haben, selbst Einfluss auf einzelne Datenverarbeitungsprozesse zu nehmen.
- Wie Nutzerinnen und Nutzer effektiv ihre Betroffenenrechte nach § 34 und § 35 BDSG ausüben können.

## **9. Datensouveränität**

Es ist sicherzustellen, dass die Nutzerinnen und Nutzer ihre Betroffenenrechte nach § 34 und § 35 BDSG (Auskunfts-, Berichtigungs- und Löschungsansprüche) angemessen wahrnehmen können.

Die Verarbeitung personenbezogener Daten der Betroffenen darf nur unter deren Kontrolle erfolgen.

Soweit externe Zugriffe, zum Beispiel im Rahmen einer Fernwartung, auf Smart Home-Anwendungen erforderlich sind, ist festzulegen, wie Nutzerinnen und Nutzer diese erkennen und unter welchen Voraussetzungen sie diese unterbinden können. Nutzerinnen und Nutzer haben das Recht, die Datenflüsse aus ihrem häuslichen Bereich zu unterbinden, unbeschadet vertraglicher Pflichten.

Im Falle eines Besitzwechsels der Smart Home-Lösung oder Beendigung des Vertragsverhältnisses muss sichergestellt sein, dass Nutzerinnen und Nutzer ihre personenbezogenen Daten löschen können. Dies betrifft sowohl die Daten, die innerhalb der Smart Home-Komponenten (Steuerungseinheiten, Sensoren usw.) gespeichert sind, als auch solche, die bei Anbietern, Herstellern oder externen Dienstleistern vorgehalten werden.

## **10. Datensparsamkeit**

Bei der Gestaltung von Smart Home-Lösungen sollte darauf geachtet werden, dass anfallende Daten möglichst ohne (direkten) Personenbezug verarbeitet werden. Dies gilt insbesondere dann, wenn die Daten außerhalb des häuslichen Bereichs verarbeitet werden.

Insbesondere bei Geräte-, Verbrauchs- und Nutzungsdaten ist ein Personenbezug häufig nicht erforderlich. Anbieter und Hersteller sollten daher bereits bei der Entwicklung ihrer Lösungen auf die Verarbeitung der Daten in personenbezogener Form verzichten, wenn dies für die Funktionalität nicht benötigt wird.

Wenn Zusatzfunktionen oder Mehrwertdienste eine Personenbeziehbarkeit voraussetzen, sollte den Nutzerinnen und Nutzern eine Wahlmöglichkeit angeboten werden. Über die bestehenden Optionen sind die Nutzerinnen und Nutzer in verständlicher Form zu informieren. Die Voreinstellungen sollten dabei auf eine datensparsame beziehungsweise pseudonyme Verarbeitung der im Rahmen der Smart Home-Lösung anfallenden Daten ausgelegt sein, so dass Änderungen bewusst vorgenommen werden müssen.

Wo aus Gründen der Funktionalität eine individuelle Zuordnung zum Beispiel von Geräte-, Verbrauchs- oder Nutzungsdaten zu bestimmten Personen unerlässlich ist, sollten pseudonyme Verarbeitungsmöglichkeiten vorgesehen werden.

Wenn im Laufe der Verarbeitung das Erfordernis einer personenbezogenen Verarbeitung entfällt, sollte zeitnah eine Anonymisierung oder Löschung erfolgen.

## **11. Kontroll- und Steuerungsmöglichkeiten für Nutzerinnen und Nutzer**

Bei der Gestaltung von Smart Home-Lösungen sollten Möglichkeiten vorgesehen werden, die es den Nutzerinnen und Nutzern erlauben, den gewünschten Funktionsumfang beziehungsweise Art und Umfang der verarbeiteten Daten selbst festzulegen und gegebenenfalls zu ändern.

Es sollten Möglichkeiten für eine Einsichtnahme der Nutzerinnen und Nutzer in die gespeicherten Daten vorhanden sein.

Es sollten Möglichkeiten zur Löschung von Geräte-, Verbrauchs- und Nutzungsdaten durch die Nutzerinnen und Nutzer vorhanden sein.

Benutzeranmeldungen, Zugriffe auf Geräte-, Verbrauchs- und Nutzungsdaten, Datenübertragungen an Stellen außerhalb des häuslichen Bereichs und die Änderung von Systemeinstellungen sollten anhand einer geeigneten, manipulationssicheren Protokollierung nachvollzogen werden können.

Soweit Smart Home-Lösungen einen Zugriff durch mehrere Benutzer ermöglichen, sollte grundsätzlich zwischen administrativen Nutzern (Installation, Konfiguration, Rechteverwaltung etc.) und sonstigen Nutzern unterschieden werden. Weiterhin sollte die Möglichkeit bestehen, Funktions- und Datenzugriffe je Nutzer unterschiedlich festlegen zu können.

## **12. Sicherheit bei Datenspeicherung, -übertragung und -zugriff**

Bei der Gestaltung von Smart Home-Lösungen ist darauf zu achten, dass alle Übertragungen personenbezogener Daten, d.h. innerhalb des häuslichen Umfeldes sowie bei der Übertragung an externe Stellen, nur über verschlüsselte Verbindungen erfolgen.

Daten aus Smart Home-Lösungen, insbesondere Geräte-, Verbrauchs- und Nutzungsdaten, sollten auf den Systemen der Anbieter/Hersteller sowie gegebenenfalls einbezogener weiterer Stellen nur in verschlüsselter Form gespeichert werden.

Datenzugriffe sowie die Änderung von System- und Benutzereinstellungen dürfen nur auf der Grundlage einer verlässlichen Authentifizierung der Benutzer beziehungsweise beteiligter Komponenten möglich sein. Bei externen Zugriffen oder der Nutzung von Online-Diensten sollte eine Zwei-Faktor-Authentifizierung genutzt werden (Gerätetoken, SMS-Authorisierungscode, Transaktionsnummer, Zertifikate etc.).

Über die Einbindung von Cloud-Diensten in die jeweilige Smart Home-Lösung sind die Nutzerinnen und Nutzer zu informieren.

Soweit Cloud-Dienste Bestandteil einer Smart Home-Lösung sind, sind die Folgen der Safe Harbor-Entscheidung des EuGH vom 6. Oktober 2015 (C-362/14) zwingend zu berücksichtigen. Auf dieser Grundlage sollte derzeit nur auf solche Dienste zurückgegriffen werden, bei denen die Speicherung und Verarbeitung der Daten von Anbietern und in Rechenzentren in der Europäischen Union beziehungsweise im

Europäischen Wirtschaftsraum erfolgt und eine Weitergabe von Daten an Stellen außerhalb dieses Bereichs verlässlich ausgeschlossen ist.

Für den Betrieb von Smart Home-Lösungen sind Verfahrensweisen festzulegen, mit denen bei Bedarf für die eingesetzten Softwarekomponenten Sicherheitsaktualisierungen vorgenommen werden können. Die Vertrauenswürdigkeit der entsprechenden Software ist vor der Installation anhand geeigneter Mechanismen zu überprüfen (Digitale Signatur/Zertifikate).

Bei Entwicklung und Betrieb von Smart Home-Lösungen sind anerkannte Standards der IT-Sicherheit und des Datenschutzes zu berücksichtigen (z.B. ISO 2700x, ISO 27018, BSI IT-Grundschutz). Dies sollte durch eine entsprechende Zertifizierung nachgewiesen werden.

Der Betrieb von Smart Home-Lösungen sollte auf der Grundlage eines IT-Sicherheits- und Datenschutzkonzepts erfolgen.

## **Empfehlungen für Verbraucherinnen und Verbraucher zur kompetenten Auswahl und Nutzung von Smart Home-Angeboten**

Der Markt für Smart Home-Lösungen ist vielfältig. Zahlreiche Hersteller und Diensteanbieter konkurrieren mit sehr unterschiedlichen Produkten. Vor dem Kauf sollten Sie Ihren konkreten Bedarf ermitteln. Dabei sollte berücksichtigt werden, welche Geräte angeschlossen werden sollen. Man sollte prüfen, ob die gewählte Produktlinie oder Geräteplattform den eigenen Anforderungen gerecht werden kann. Außerdem müssen die baulichen Eigenschaften Ihres Zuhauses die Voraussetzungen für den Einbau des jeweiligen Systems erfüllen. Möglicherweise müssen zum Beispiel Leitungen verlegt, Funkverbindungen eingerichtet oder Schalter in Wände eingebaut werden.

Wer die Smart Home-Anlage schrittweise erweitern möchte, sollte den Zustand nach dem vollständigen Ausbau im Blick haben und entsprechende Grundlagen legen. Von Beginn an sollten die Ausbauschnitte so gestaltet sein, dass sie die gewünschten Erweiterungen zulassen. Fachbetriebe, Hersteller und Einzelhändler beraten Sie im Vorfeld und unterstützen Sie bei der Planung.

### **1. Installation und Inbetriebnahme**

Es gibt Smart Home-Geräte und -Dienste, die durch Sie selbst installiert werden können, andere erfordern die Installation durch einen Fachbetrieb. Wenn Sie sich für ein Produkt zur Selbstinstallation entscheiden, achten Sie darauf, dass die Installationsanleitung den Produkten in gedruckter Form beigelegt ist und sich diese auf die aktuelle Revision beziehungsweise Version eines Produktes bezieht. Achten Sie darauf, dass dazu gegebenenfalls auch neue Betriebsanleitungen kostenfrei zum Download zur Verfügung gestellt werden.

Ändern Sie voreingestellte Passwörter und verwenden Sie ein möglichst sicheres Passwort (mit hoher Zeichenanzahl, wechselnder Groß-/Kleinschreibung, mehreren Ziffern, Sonderzeichen).

Bei der Inbetriebnahme könnten von Ihnen zahlreiche persönliche Daten abgefragt werden, die zum Betrieb der Smart Home-Funktionen nicht erforderlich sind. Grundsätzlich ist es ratsam, möglichst wenige Daten preiszugeben.

### **2. Geräteeigenschaften**

Funkgesteuerte Geräte haben nur eine begrenzte Reichweite, die je nach baulichen und anderen Gegebenheiten unterschiedlich sein kann. In den Produktinformationen der Hersteller finden sich häufig Angaben zur theoretischen Funkreichweite unter optimalen Bedingungen. Beachten Sie, dass die tatsächliche Reichweite und die

Zuverlässigkeit aufgrund der baulichen Gegebenheiten und äußerer Störeinflüsse deutlich von den Angaben abweichen können. Störeinflüsse können sich zudem jederzeit ändern.

Informieren Sie sich nach Möglichkeit über den Energieverbrauch der Geräte. Sie sollten einen möglichst geringen Verbrauch aufweisen, insbesondere im Bereitschaftszustand. Bei batteriebetriebenen Geräten erkundigen Sie sich vor dem Kauf nach dem Batterietyp, der erwartbaren Batterielebensdauer und möglichen Folgekosten.

Viele Smart Home-Geräte und -Dienste können durch Service-Techniker aus der Ferne über das Internet gewartet werden. Dazu nehmen sie von außen mit den installierten Geräten oder Diensten Kontakt auf. Ein Zugriff sollte nur nach Ihrer ausdrücklichen Einwilligung und begrenzt auf den jeweiligen Fall möglich sein. Von der Möglichkeit der Fernwartung können Sie vereinzelt auch dann Gebrauch machen, wenn Sie bei der Einrichtung oder Bedienung auf Probleme stoßen.

### **3. Bedienung**

Wer Smart Home-Anwendungen nutzt, möchte in der Regel allen Familienmitgliedern die Bedienung der verschiedenen Smart Home-Geräte und -Dienste erlauben. Allerdings sollten nicht alle Nutzerinnen und Nutzer über alle verfügbaren Zugriffsrechte verfügen. Achten Sie bei der Auswahl der Smart Home-Geräte und -Dienste darauf, dass Sie verschiedene Benutzerkonten mit unterschiedlichen Berechtigungen einrichten können. Damit kann zum Beispiel vermieden werden, dass jeder Nutzer Änderungen an den Grundeinstellungen des Systems vornehmen kann.

Wenn Sie technische Unterstützung benötigen, können Sie sich an Ihren Händler oder den Fachbetrieb wenden, der die Geräte installiert hat. Teilweise bieten auch die Hersteller der Geräte oder Betreiber von Diensten eine Hilfestellung an. Informieren Sie sich, welche Kontaktmöglichkeiten zum Anbieter bestehen, zum Beispiel telefonisch, persönlich, per E-Mail, per Web-Chat, Fernwartung und in Form von Hilfetexten (sog. FAQs) im Internet.

Die technische Unterstützung sollte für Sie idealerweise kostenlos oder nur mit geringen Entgelten verbunden sein.

Halten Sie die Betriebssoftware und die entsprechenden Apps aktuell, laden Sie regelmäßig die Updates herunter oder nutzen Sie Funktionen, mit denen die Updates automatisch eingespielt werden. Updates dienen in der Regel der Erhöhung der Sicherheit oder verändern den Funktionsumfang. Prüfen Sie, dass nach dem Einspielen von Updates die System- und Datenschutzeinstellungen wieder Ihren Wünschen entsprechen. Ein Update kann Auswirkungen auf das Zusammenspiel von einzelnen Geräten, die Interoperabilität, haben. Achten Sie daher darauf, dass eine Möglichkeit vorhanden ist, mit welcher der vorherige Zustand wiederhergestellt werden kann.

#### **4. Kosten und Vertragsmodelle**

Die Nutzung von Smart Home-Geräten oder -Diensten kann mit Zusatzkosten verbunden sein. Informieren Sie sich über mögliche weitere Rechnungsposten, die einmalig, regelmäßig oder nutzungsabhängig anfallen, so zum Beispiel wenn die Grundfunktionen nur mittels Anbindung an das Internet oder durch die Nutzung von Cloud-Diensten genutzt werden können.

Falls der Anbieter kostenpflichtige Zusatzdienste in einem Abonnement-Modell anbietet, achten Sie am besten auf kurze Mindestvertragslaufzeiten. Damit haben Sie die Möglichkeit, flexibel auf das Angebot eines anderen Unternehmens umzusteigen, wobei die technischen Voraussetzungen geprüft werden sollten. Sollten Ihnen Geräte im Rahmen eines Mietvertrages überlassen werden, ist es ratsam, die Kosten für den Kauf der Geräte und die Kosten der Miete für mehrere Jahre gegenüberzustellen. Möglicherweise lohnt sich der Kauf.

Sie sollten darauf achten, dass Informationen zu Entgelten und Vertragsbedingungen vollständig und in übersichtlicher Weise auf der Homepage der Anbieter im Internet abrufbar sind.

#### **5. Interoperabilität und Erweiterbarkeit**

Smart Home-Anwendungen nutzen verschiedene Schnittstellen und arbeiten deswegen nicht immer zusammen, d.h. sie sind nicht zwingend kompatibel beziehungsweise interoperabel.

Informieren Sie sich als Anwenderin oder Anwender über die Interoperabilität unterschiedlicher Geräte und Systeme auf den Internetseiten oder beim Anbieter direkt.

Damit Smart Home-Lösungen auch auf wechselnde Bedürfnisse eingestellt werden können, sollten Sie darauf achten, dass installierte Systeme mit neuen Geräten erweitert werden können. Beachten Sie, dass manche Systeme nicht mit Geräten anderer Hersteller ergänzt werden können.

#### **6. Haltbarkeit**

Die Anbieter, für die Sie sich entscheiden, sollten für ihre Geräte und Dienste eine möglichst lange Lebensdauer vorsehen. Dazu gehören insbesondere technische Hilfe, die Versorgung mit Ersatzteilen und die Bereitstellung von Sicherheitsupdates. Ist dies nicht der Fall, könnte ein Smart Home-System schnell in Teilen oder ganz unbrauchbar werden. Erkundigen Sie sich deswegen nach den Zeiträumen, die für die technische Unterstützung vorgesehen sind.

## **7. Personenbezug und grundsätzliche Zweckbindung von Daten**

Smart Home-Anwendungen bringen für Sie als Verbraucherin und Verbraucher erhebliche Vorteile mit sich und können dazu beitragen, Ihren häuslichen Alltag in vielfältiger Hinsicht zu erleichtern.

Sie sollten sich allerdings darüber bewusst sein, dass eine Vielzahl von Smart Home-Lösungen personenbezogene Daten erheben. Auch auf den ersten Blick rein technische Daten – wie zum Beispiel die Sensorwerte Ihrer Heizung – können (Dritten) mitunter tiefe Einblicke in Ihren Lebensalltag gewähren. Die Heizungswerte können so zum Beispiel das Nutzungsverhalten in Bezug auf einzelne Räume recht genau offenbaren.

Um Ihre Privatsphäre effektiv schützen zu können, sollten Sie sich daher bereits beim Erwerb einer Smart Home-Lösung darüber informieren, welche Daten über Sie erhoben und verarbeitet werden sollen und welcher Zweck damit verfolgt wird. Grundsätzlich gilt dabei, dass das geltende Datenschutzrecht nur solche Datenverarbeitungen erlaubt, die für den Betrieb der von Ihnen gewählten Smart Home-Lösung tatsächlich erforderlich sind und nicht über den vertraglich vereinbarten Umfang hinausgehen.

Wofür ein Smart Home-Anbieter Daten über Sie verwenden darf, folgt also in erster Linie aus dem mit Ihnen geschlossenen Vertrag. Wenn der Anbieter darüber hinaus personenbezogene Daten verarbeiten möchte (z.B. die Weitergabe an Dritte), benötigt er hierzu regelmäßig Ihre ausdrückliche Einwilligung. Wird eine solche von Ihnen verlangt, sollten Sie darauf achten, dass Sie durch ausreichende und verständliche Informationen in die Lage versetzt werden, die Folgen Ihrer Einwilligungserklärung abschätzen zu können.

## **8. Transparenz der Datenverwendung**

Beim Erwerb einer Smart Home-Lösung sollten Sie darauf achten, dass Sie bereits vor deren ersten Inbetriebnahme transparent und für Sie nachvollziehbar darüber unterrichtet werden, welche Sie betreffende Daten verarbeitet werden sollen. Es empfiehlt sich insoweit, auf die folgenden Punkte ein besonderes Augenmerk zu legen:

- Welche personenbezogenen Daten werden auf welcher Rechtsgrundlage, in welchem Umfang, in welcher Weise und zu welchem Zweck verarbeitet? Welche Daten sind dabei zur Erfüllung des Vertragszwecks wirklich erforderlich und welche gegebenenfalls zu anderen Zwecken?
- Wer ist für die einzelne Datenverwendung verantwortlich? Werden Dritte bei der Vertragserfüllung mit einbezogen? Erfolgt die Datenverarbeitung nach europäischen Datenschutzstandards (z.B. innerhalb der EU)?
- Ob und in welchem Umfang besteht die Möglichkeit, selbst Einfluss auf die Datenverwendung zu nehmen, und welchen Einfluss hat dies auf den Funktionsumfang?



## **9. Datensouveränität**

Sie sollten bei der Nutzung von Smart Home-Anwendungen darauf achten, dass Sie die Kontrolle über die stattfindenden Datenverarbeitungsprozesse behalten. Sie können sich dabei von den folgenden Fragen leiten lassen:

- Wie und bei welcher Stelle können effektiv datenschutzrechtliche Betroffenenrechte (Auskunftsanspruch oder Löschungsanspruch) geltend gemacht werden?
- Ob und inwieweit sind externe Zugriffe durch die Anbieter einer Smart Home-Anwendung – zum Beispiel im Rahmen der Fernwartung – notwendig? Wie können diese erkannt und unter welchen Voraussetzungen unterbunden werden?
- Ob und unter welchen Voraussetzungen können Datenflüsse aus Ihrem häuslichen Bereich unterbunden werden und welche (z.B. vertragsrechtlichen) Folgen können damit verbunden sein?
- Ob und inwieweit ist die Datenlöschung bei einem Besitzwechsel an der Smart Home-Lösung oder der Beendigung des Vertragsverhältnisses möglich? Denken Sie dabei nicht nur an die Daten, die auf den einzelnen Smart Home-Komponenten wie zum Beispiel der Steuerungseinheit oder den Sensoren angefallen sind, sondern auch an die bei Anbietern, Herstellern oder externen Dienstleistern gespeicherten Daten.

## **10. Datensparsamkeit**

Die im Zusammenhang mit Smart Home-Lösungen anfallenden Geräte-, Verbrauchs- oder Nutzungsdaten erlauben unter Umständen tiefgehende Einblicke in Ihre private Lebensgestaltung oder Ihr persönliches Verhalten. Insbesondere dann, wenn externe Stellen in die Verarbeitung dieser Daten einbezogen sind, sollte ein direkter Personenbezug daher vermieden werden können.

Bei der Auswahl von Smart Home-Lösungen sollten Sie daher darauf achten, dass eine pseudonyme oder anonyme Datenverarbeitung möglich ist. Bei einer pseudonymen Verarbeitung können zum Beispiel individuelle Zuordnungen oder Auswertungen erfolgen, ohne dass aus den Daten die betroffene Person unmittelbar erkennbar ist. Bei einer Anonymisierung können die Daten nicht mehr oder nur mit unverhältnismäßigem Aufwand einer bestimmten Person zugeordnet werden.

In die Auswahlentscheidung sollte deswegen die Überlegung einbezogen werden, ob der Anbieter/Hersteller eine Pseudonymisierung oder Anonymisierung zumindest optional anbietet.

## **11. Kontroll- und Steuerungsmöglichkeiten für Nutzerinnen und Nutzer**

Bei der Auswahl von Smart Home-Lösungen sollten Sie prüfen, ob je nach Art der Lösung folgende Möglichkeiten bestehen:

- Funktionsumfang sowie Art und Umfang der zu verarbeitenden Daten können von Ihnen festgelegt und gegebenenfalls geändert werden.
- Sie können die gespeicherten Daten einsehen und Geräte-, Verbrauchs- und Nutzungsdaten bei Bedarf löschen.
- Benutzeranmeldungen, Datenzugriffe, Datenübertragungen an Stellen außerhalb des häuslichen Bereichs und Änderungen von Einstellungen lassen sich anhand einer Protokollierung nachvollziehen.
- Die Lösung unterscheidet zwischen administrativen Nutzern mit besonderen Berechtigungen (z.B. für die Installation und Konfiguration) und sonstigen Nutzern.
- Funktions- und Datenzugriffe können je Nutzer unterschiedlich festgelegt werden.

## **12. Sicherheit bei Datenspeicherung, -übertragung und -zugriff**

Bei der Auswahl von Smart Home-Lösungen sollten Sie prüfen, ob je nach Art der Lösung folgenden Aspekten entsprochen wird:

- Datenübertragungen erfolgen über verschlüsselte Verbindungen.
- Geräte-, Verbrauchs- und Nutzungsdaten werden verschlüsselt gespeichert.
- Datenzugriffe und die Änderung von Einstellungen sind erst nach einer verlässlichen Authentifizierung möglich (z.B. Zugangskennung/Passwort).
- Bei Cloud-Diensten erfolgt die Speicherung und Verarbeitung personenbezogener Daten bei Anbietern und in Rechenzentren in der Europäischen Union beziehungsweise im Europäischen Wirtschaftsraum.
- Seitens des Anbieters/Herstellers werden regelmäßige Sicherheitsaktualisierungen der eingesetzten Software der Komponenten, also auch etwaiger Apps, angeboten.
- Es wird durch eine Zertifizierung nachgewiesen, dass bei Entwicklung und Betrieb anerkannte Standards der IT-Sicherheit und des Datenschutzes berücksichtigt werden.