VVB magazin

6/2018
Erscheint 6 x im Jahr
Einzelheft € 5,-
53. Jahrgang
15. Dezember 2018


Vier interessante Referate:

# Nach IDD ist vor LVRG II

Herbsttagung des Fachkreises
Marketing/Vertrieb bei der ERGO in Düsseldorf

Bericht ab Seite 174

SAVE THE DATE
24./25. MAI 2019

Mitgliederversammlung 2019
MÜNSTER

**Treffpunkte:**
TP Köln besucht St. Severin

**ivwKöln:**
Ehrung der Absolventen, Begrüßung der Neuen, Fächervorstellung, Exkursion nach Baden-Baden

**Fachthema:**
DSGVO und Smart Home

**VVBintern:**
Lehrgang „R“ auf Reisen

**Interview:**
25 Fragen an Olaf Bläser

# Auswirkungen der EU-DSGVO im Smart Home

von PIRMIN SCHÄFER (kor. M.)

## Einleitung

Versicherungsunternehmen in Deutschland haben die Innovationskraft und Umsatzpotenziale im Wirtschaftszweig „Internet der Dinge“ erkannt und wollen sie nutzen. Sie beginnen ihre traditionellen Produkte der Hausratversicherung mit versicherungsbezogenen Komponenten des **Smart Livings** zu kombinieren. Ihre Absicht ist es, durch den Zugang zu den erhobenen Daten den Privatkunden als mathematisch kalkuliertes Versicherungsindividuum besser zu verstehen, durch passende Assistance-Leistungen den Komfort und die Sicherheit des Kunden zu erhöhen und im Resultat sowie mit Hilfe von Subvention der technischen Grundausstattung die Loyalität des Kunden zu steigern. Darüber hinaus verfolgen sie mit solchen Bündelprodukten das Ziel, aus dem bisher kurativ geprägten Versicherungsmodell auszubrechen und die Prävention von Schäden in den Mittelpunkt zu stellen.

**Smart Home** dient als Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt eine **Erhöhung** von **Wohn- und Lebensqualität, Sicherheit** und **effizienter Energienutzung** auf Basis **vernetzter** und **fernsteuerbarer** Geräte und Installationen sowie **automatisierbarer** Abläufe steht.
*Quelle: Bitkom Deloitte 2011*

Mit der am 25. Mai 2018 wirksam gewordenen europäischen Datenschutz-Grundverordnung (EU-DSGVO) gibt es erstmals einen europaweit einheitlichen Rahmen für die Verarbeitung personenbezogener Daten. Nahezu alle Wirtschaftsbereiche haben Anpassungen vorzunehmen, da fast überall in zumindest kleinem Umfang personenbezogene Daten verarbeitet werden. So sind auch Innovationsthemen wie das Internet der Dinge, und im vorliegenden Fall, das Smart Home als intelligent vernetztes Heim betroffen. Hersteller und Anbieter dieser Produkte sind bei der Ergreifung geeigneter Maßnahmen zur Einhaltung der Bestimmungen zunächst auf sich allein gestellt, da die zuständigen Bundes- und Landesbehörden erst peu à peu Richtlinien, Checkliste und Leitfäden herausgeben. Der vorliegende Artikel befasst sich mit den konkreten Auswirkungen der Datenschutzgrundverordnung im Smart Home und liefert damit einen Beitrag zur datenschutzkonformen Gestaltung dieser Produkte und Dienstleistungen.

Die individuellen Bedürfnisse nach **Sicherheit, Komfort** und **Effizienz** bringen es zwangsläufig mit sich, dass personenbezogene Daten erfasst werden müssen, wenn im Zuge der Planung, Errichtung oder Modernisierung sowie beim Unterhalt des eigenen geschickt vernetzten und komfortabel gesteuerten Heims intelligent vernetzte Geräte installiert werden. Diese Daten werden von Sensoren gemessen, oft auf IoT-Plattformen aggregiert und im weiteren Verlauf an den Hersteller und/oder einen dritten Dienstleister wie z.B. ein Versicherungsunternehmen übermittelt.

**Personenbezogene Daten** (englisch: Personally identifiable information, PII) definiert die DSGVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. So lässt sich direkt oder indirekt mit Merkmalen, die etwa im persönlichen Umfeld wie der eigenen Wohnung generiert wurden und Ausdruck der Identität dieser natürlichen Person sind, mit vertretbarem Aufwand ein Bezug zu ihr herstellen. Neben allgemeinen Merkmalen wie Name, Stimme oder Kreditkartennummer und zählen beispielsweise auch eher technische Attribute wie IP-Adressen, GPS-Daten oder persönliche Geräteeinstellungen zu den personenbezogenen Daten.

## Datenschutzbegriff und DSGVO

Der Datenschutzbegriff entwickelte je nach Betrachtungsweise im Laufe der Zeit die heute gebräuchlichen vier Säulen des Schutzaspektes heraus (siehe Grafik 1: Vier Säulen des Datenschutzrechts).

Die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ hat die in Grafik 2 dargestellte grundlegende Struktur.

## Anwendbarkeit der DSGVO für das Smart Home

Nach den allgemeinen Bestimmungen in Artikel 1 behandeln die folgenden Artikel 2 und 3 sachliche und räumliche Anwendungsbereiche der Verordnung und nehmen dabei Bezug auf eine ganz, teilweise oder nicht automatisierte „**Verarbeitung personenbezogener Daten**“ [Art. 2 Abs. 1 DSGVO] von EU-Bürgern. Dieser Vorgang, darunter fallen u.a. das Erheben, Speichern, Verändern, Auswerten, Übermitteln oder Löschen von Daten, ist „unabhängig davon, ob die Verarbeitung in der Union stattfindet“ [Art. 3 Abs. 1 DSGVO]. Gemäß dem **Marktortprinzip** (und nicht dem Territorial- oder Herkunftslandprinzip) ist für die Anwendung der Verordnung einzig relevant, dass „betroffenen Personen in der Union Waren oder Dienstleistungen“ [Art. 3 Abs. 2 lit. a DSGVO] mit oder ohne einer Zahlungsleistung angeboten werden oder ihr Verhalten innerhalb der EU beobachtet wird.

Zweifel an der Anwendbarkeit bestehen, wenn sich eine „persönliche und familiäre Sphäre“ [Vgl. Grafenstein in: Gierschmann (2018) 2018 S. 36, Rn. 50] mit dem öffentlichen Raum überschneidet, wie dies bei der personenbezogenen Datenerhebung durch Videokameras im Eingangsbereich von Privathäusern der Fall sein kann.

Artikel 5 und 6, mit denen das zweite Kapitel beginnt, verweisen für die praktische Auslegung der Grundsätze für die Verarbeitung personenbezogener Daten auf den auf die Verhältnismäßigkeit abzielenden Lauterkeitsgrundsatz „Treu und Glauben" im Sinne von Fairness und damit einhergehende Prinzipien wie

- **Rechtmäßigkeit**,
- **Transparenz,**
- **Zweckbindung,**
- Begrenzung der Speichermenge (**Datenminimierung)** sowie Speicherdauer,
- Richtigkeit im Sinne einer „Repräsentation der Realität",
- Schutz vor Missbrauch und Verlust durch **Integrität** und **Vertraulichkeit** sowie
- die **Rechenschaftspflicht**.

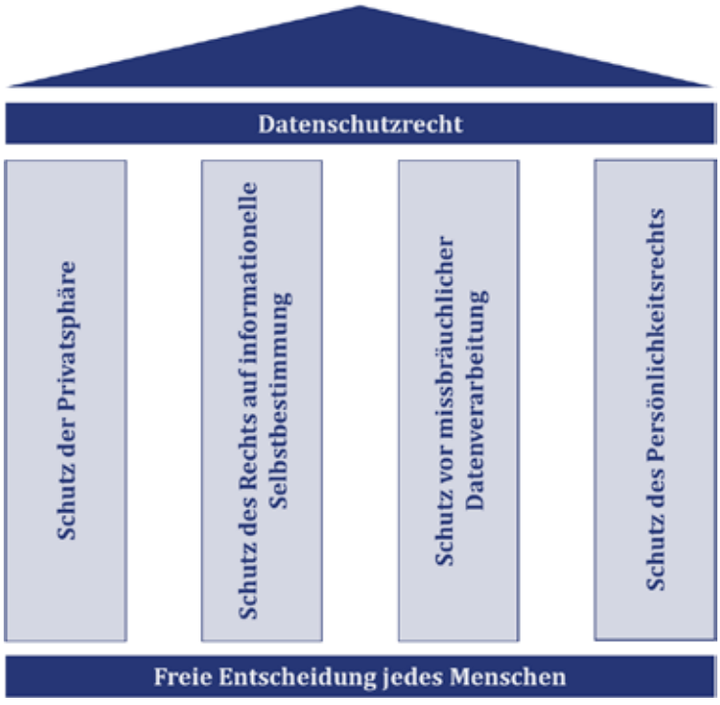
Speziell die beiden Grundsätze der „qualitativ und quantitativ begrenzte[n]" [Frenzel in: Paal/Pauly (2017) S. 79, Rn. 34] Datenminimierung und Speicherdauer spielen neben der Verknüpfung zur Zweckbindung schon aus Gründen der effizienten Nutzung von begrenzten Rechen- und Speicherkapazitäten einzelner Komponenten im Smart Home eine entscheidende Rolle. Eine ausreichend hohe Internetbandbreite vorausgesetzt, kann alternativ auf Ressourcen in der Cloud zurückgegriffen werden. Eine technische Lösung, die beide Welten des **Cloud-Computings** und der lokalen Datenverarbeitung auf sogenannten Fat Clients vereint, stellt das Prinzip des **Edge Computings** dar. Es sieht vor, dass nicht die erfassten personenbezogenen Daten selbst, sondern nur das aggregierte, berechnete oder abgeleitete, möglicherweise auch **pseudonymisierte** und damit weniger für Datenschutzbestimmungen anfällige Ergebnis vom Erfassungsgerät an vernetzte Stellen übertragen wird.

Schutz vor Missbrauch und Verlust durch Einhaltung eines angemessenen Maßes an Integrität und Vertraulichkeit kann im Smart Home durch **Authentifizierungsmethoden** in Zugangsbereichen wie Haustüren und Garagen- oder Gartentoren und aufeinander abgestimmte, regelmäßig ausgeführte Datenbackupkonzepte auf sichere Speichermedien realisiert werden.

Artikel 7 folgend, ist der Verantwortliche verpflichtet, eine Einwilligung für die Verarbeitung personenbezogener Daten einer betroffenen Person vorweisen zu können, für die zuvor „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" [Art. 7 Abs. 2 DSGVO] Datenschutzregeln formuliert wurden, sodass die Einwilligung von der betroffenen Person jederzeit genau „so einfach" widerrufen werden kann. Gleichzeitig muss die Einwilligung freiwillig erfolgt sein und darf an keine andere für die Vertragserfüllung nicht erforderliche Verarbeitung geknüpft sein („**Koppelungsverbot**").

Wenn Kinder in einem Smart Home aufwachsen, so müssen die Erziehungsberechtigten bei ihren Schützlingen von Beginn an für ein gesundes Maß und ein angemessenes Verständnis für die im Haus verbaute Technik sorgen. Nur so können **Minderjährige** für sich entscheiden, welche Dinge sie in ihrer privaten Freizeit tun und welche Folgen dies im Hinblick auf etwaige Lausch-, Überwachungs- oder Sicherheitsinstallationen im Wohnbereich haben kann. Kinder sind also besonders davor zu schützen, wenn das Smart Home von ihnen personenbezogene Daten erzeugt. Gleichzeitig ist aber auch das Smart Home vor Kindern zu schützen. Dies gilt für den Fall, dass sie wissentlich oder unwissentlich Einstellungen oder Geräte manipulieren oder beschädigen.

In den zwölf Artikeln des dritten Kapitels




*Grafik 1: Vier Säulen des Datenschutzrechts*

*Grafik 2: Struktur der EU-DSGVO*

stehen die **Betroffenenrechte** im Mittelpunkt, die der betroffenen Person „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“ [Art. 12 Abs. 1 DSGVO] sind.

Ferner ist die betroffene Person über die Begründung von **berechtigten Interessen** des Verantwortlichen, ihre Betroffenenrechte sowie über den Anlass der Bereitstellung zu informieren. Zur Vereinfachung dürfen dazu „leicht ... verständliche“ [Art. 12 Abs. 7 DSGVO], standardisierte und somit in digitaler Form auch maschinenlesbare Piktogramme eingesetzt werden, durch die „die betroffene Person bereits auf den ersten Blick einen Überblick über die beabsichtigte Verarbeitung erhalten“ [Paal/Hennemann in: Paal/Pauly (2017) S. 173, Rn. 75] kann. In Grafik 3 sind die in diesem Kapitel behandelten Betroffenenrechte zusammengestellt.

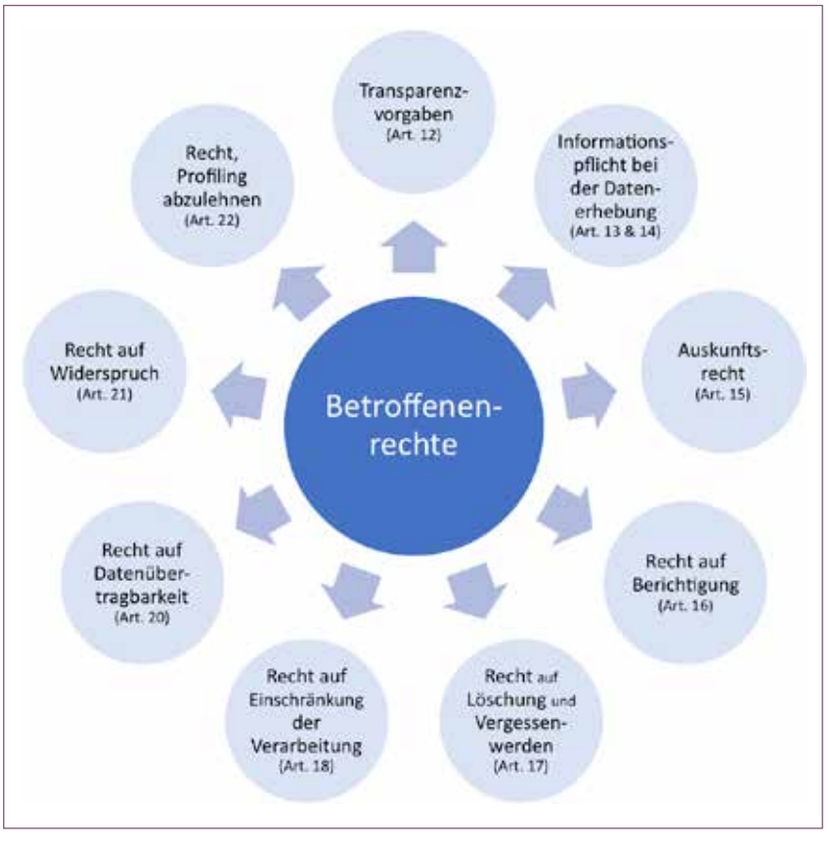
Für Smart-Home-Kunden ist hier musterhaft eine zentrale, intranetbasierte „Datenschutz-Plattform“ denkbar, die alle im Haus verbauten Smart Devices in übersichtlicher Form nach Zweck oder Funktion gruppiert. Die Anwender könnten auf diese Weise einsehen,

- welche Daten bzgl. Art und Inhalt von ihnen erfasst werden,
- auf welche Weise und für welchen Zweck sie verarbeitet werden und
- wohin sie übermittelt werden.

Die Neuerung bei einer solchen Steuerungszentrale wäre nicht nur, dass selbstverständlich sämtliche Datenströme und Datenträger mit state-of-the-art-Technology („**Stand der Technik**“) end-to-end verschlüsselt würden, sondern der Nutzer alle Daten auf einen Blick sähe und attributsspezifisch Einstellungen dazu vornehmen könnte, z.B.:

1. Einwilligung erteilen und entziehen,
2. Speicher- und Nutzungsdauer anpassen,
3. Zweckbestimmung verändern,
4. Widersprüche einlegen,
5. Auskünfte beim Anbieter oder Hersteller anfordern (z.B. historisierter, statistisch-stochastischer Datenabzug),
6. Erteilung der Verarbeitungserlaubnis für vom Hersteller angefragte Zwecke, ggf. gegen Gebühr (erstmals selbstbestimmter Verkauf eigener Daten).

Neben der Unterrichtung über ihre Betroffenenrechte muss der Verantwortliche gegenüber der betroffenen Person außerdem




*Grafik 3: Betroffenenrechte gemäß der EU-DSGVO*

„die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung“ im Falle der Verwendung „einer **automatisierten Entscheidungsfindung** einschließlich Profiling“ [Art. 13 Abs. 2 lit. f DSGVO] transparent machen. Beim Einsatz künstlicher neuronaler Netze, speziell bei Seed-AI, also **künstlicher Intelligenz (KI)**, die sich durch Rekursion eigenständig verbessert und erweitert, stellt sich die Frage, wie „der konkrete Prozess der Entscheidungsfindung ... für ... steuernde Instanzen ... [oder] Betroffene eindeutig prognostizierbar“ [Wischmeyer (2018): Regulierung intelligenter Systeme S. 44] ist.

Auch Artikel 15 misst gemeinsam mit Erwägungsgrund 63 dem **Auskunftsrecht** der betroffenen Person einen hohen Stellenwert bei. Auf Nachfrage der betroffenen Person ist der Verantwortliche verpflichtet, offen zu legen, um welche Kategorien personenbezogener Daten es sich handelt und welche Informationen zur Herkunft der Daten vorliegen, wenn sie „nicht bei der betroffenen Person erhoben“ [Art. 15 Abs. 1 lit. g DSGVO] wurden. Besonders Auskünfte über die Speicherdauer und den Einsatz von **Profiling-Algorithmen** sind zum einen für Anbieter von Smart-Home-Versicherungstarifen relevant, die ein Produkt und die dazu passende Versicherung im Bündel vertreiben und somit auch die für die Vertragserfüllung gewünschte Zuordnung zwischen Kunde und Gerät vornehmen wollen. Zum andern spielt dies auch bei anderen Anbietern oder reinen Herstellern von Smart-Home-Produkten eine Rolle, sofern sich Geräte-IDs mit dem (registrierten) Kunden verknüpfen lassen.

Ferner gilt das „**Recht auf Vergessenwerden**“ [Vgl. ErwG 65 und ErwG 66] als „konsequente Weiterentwicklung der Löschpflicht“ [Wybitul (2017) S. 331, Rn. 19], wenn die betroffene Person gegen die Verarbeitung widersprochen hat oder durch Widerruf ihrer Einwilligung zum Ausdruck bringt, dass Daten über sie vergessen werden sollen. Wie hoch der vertretbare Aufwand für die einwandfreie Umsetzung dieser Gesetzesvorgaben anzusetzen ist, ist nach den verfügbaren Technologien und ihren Implementierungskosten, d.h. nach den „zur Verfügung stehenden Mittel[n]“ [ErwG 66 DSGVO] zu beurteilen und bietet somit er-

heblichen Interpretationsspielraum aus Sicht von Verbrauchern, Behörden und Smart-Home-Dienstleistern.

Artikel 20 verlangt für die Umsetzung des Rechts auf **Datenübertragbarkeit**, dass „personenbezogenen Daten, die [die betroffene Person] einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format" zugänglich gemacht und bei technischer Machbarkeit auch an einen neuen Verantwortlichen im Auftrag übertragen werden müssen. Bei der hier geforderten und zu fördernden **internen und externen Interoperabilität** ist keine explizite Rede davon, dass diese Übermittlung sicher, d.h. verschlüsselt, auf dem Stand der Technik erfolgen soll. Dies ist in Anbetracht eines wahrscheinlichen Versands über das Internet allerdings angebracht und technisch-organisatorisch zumutbar. Das Recht auf **Datenportabilität** verfolgt auch wettbewerb(srecht)liche Zwecke, da es versucht, **„Lock-in"-Effekte** zu reduzieren, also Nutzer davor zu schützen, dass Anbieter ihre Marktmacht durch proprietäre Formate ausnutzen und dadurch die selbstbestimmte Kontrolle durch den Nutzer unterbinden.

Eine weiterreichende Bedeutung kommt Artikel 22 zu, in dem es darum geht, dass eine „automatisierte Verarbeitung – einschließlich **Profiling** - [der betroffenen Person] gegenüber **[keine] rechtliche Wirkung** entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." [Art. 22 Abs. 1 DSGVO]. Im Kontext Smart Home, wo z.B. das Konsumverhalten über smarte Lautsprecher (vgl. Amazon Echo, Google Home, Apple HomePod, Microsoft Cortana oder Samsung Bixby) aufgezeichnet wird, ließen sich in Kombination mit der Vorschadenhistorie oder Gesundheitsparametern nach oben oder unten angepasste Tarifprämien oder Entschädigungszahlungen ableiten.

Das Prinzip der datenschutzgerechten Technikausgestaltung („**privacy by design**") gebietet, dass der Schutz **informationeller Selbstbestimmung** bereits in die (Software-) architektonische Konzipierung und anschließende Programmierung integriert wird. Datenschutz durch Voreinstellung („**privacy by default**") soll die zweckbestimmte Verarbeitung gemäß dem Grundsatz der Datenvermeidung auf das erforderliche Maß begrenzen und somit helfen, dem „ökonomisch nachvollziehbaren Wunsch [moderner Big-Data-Dienstleister] nach einer Maximierung von Datenströmen" [Martini in: Paal/Pauly (2017) S. 322, Rn. 12] entgegenzuwirken. Gleichzeitig trägt das Prinzip hinsichtlich des sogenannten Privacy Paradoxes dazu bei, „die privatsphärengeneigte Grundhaltung der Nutzer und ihr [dazu oft konträres] Nutzungsverhalten zu synchronisieren". [Martini in: Paal/Pauly (2017) S. 323, Rn. 12]

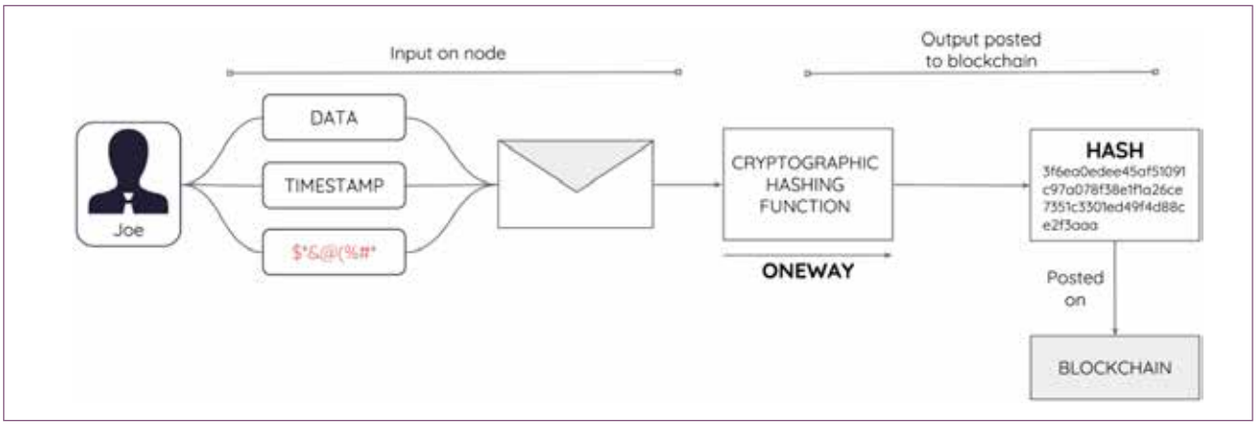
Im Sinne der Datensparsamkeit soll die Menge der Informationen demnach auf ein möglichst geringes Maß reduziert werden, womit im Vergleich zur in Art. 32 beschriebenen Datensicherheit bereits ein Schritt davor angesetzt wird. Praktische Implementierungen hierfür sind etwa **Anonymisierung** mittels Datenaggregation und **Datenminimierung** durch Single-Sign-On-Services, bei denen nur der erste Dienstleister in der Prozesskette die Nutzerauthentifizierung vornimmt. Ein innovativer Weg, sowohl **Transparenz** bei Transaktionen, als auch die Möglichkeit einer Löschung („Recht auf Vergessenwerden") in einer per Design unveränderlichen **Blockchain** abzubilden, stellen die von LegalThings One entwickelten LiveContracts dar. Durch die Kombination einer personenbezogenen Information mit einem Zeitstempel und einem Zufallswert sowie anschließendem **Hashing** wird statt einer Einzelinformation eine Art verschlüsselter Umschlag in die Blockchain geschrieben. Der Inhalt dieses Umschlags kann im Gegensatz zu seiner festen Referenz in der Kette jederzeit verändert werden. Die in Grafik 4 dargestellte Prozesskette veranschaulicht das Verfahren.

Auf Vorschlag der europäischen Agentur für Netz- und Informationssicherheit, kurz ENISA, sollen Verantwortliche ihre Produkte schon bei der Konzeptionierung auf technische und organisatorische **Möglichkeiten des Eingreifens** (englisch: „intervenability") und die Kontrolle durch den Benutzer ausrichten. Dies lässt sich auf den Grundgedanken der **informationellen Selbstbestimmung** zurückführen, wie er von Wilhelm Steinmüller und Bernd Lutterbeck 1971 formuliert wurde. Die Handlungsfreiheit, eingreifen und selbst die Kontrolle über die Informationen übernehmen zu können, bedeutet im Smart-Home-Umfeld, dass zeitweise oder dauerhaft bestimmte Sensoren, die datenschutzrelevante Daten erfassen, deaktiviert werden können müssen, wenn z.B. Gäste des Hauses dies wünschen.

Erst durch wirksame, nachprüfbare und nachvollziehbare **Sicherheitsmaßnahmen** seitens der Hersteller und Anbieter von Smart-Home-Geräten und Infrastruktur kann beim Verbraucher Vertrauen in Betreiber und Produkte entstehen. Laut Arne Schönbohm, Präsident des BSI, ist IT-Sicherheit die „Voraussetzung für das Gelingen der **Digitalisierung**" und daher kein „Kostenfaktor, sondern ein ... ‚**business enabler**' " [BSI (2017): Lage der IT-Sicherheit in Deutschland S. 15 (Kap. 1.3) und S. 77 (Kap. 3)], d.h. ermöglicht erst, eine **nachhaltige** Geschäfts- oder Kundenbeziehung aufzubauen.

*M.Sc. Pirmin Schäfer*

*Pirmin Schäfer ist Wirtschaftsinformatiker und als Senior Consultant für die DYNACON GmbH tätig. Nach seinem dualen Studium der Wirtschaftsinformatik (Bachelor) nahm er einige Jahre später ein weiteres berufsbegleitendes Studium im Fach IT-Management (Master) auf, das er zum Herbst 2018 erfolgreich abschloss. Als Teil des interdisziplinären Beraterteams der DYNACON GmbH vereint er Knowhow in Business und IT, Expertise in Data Analytics und Umsetzungsstärke.*

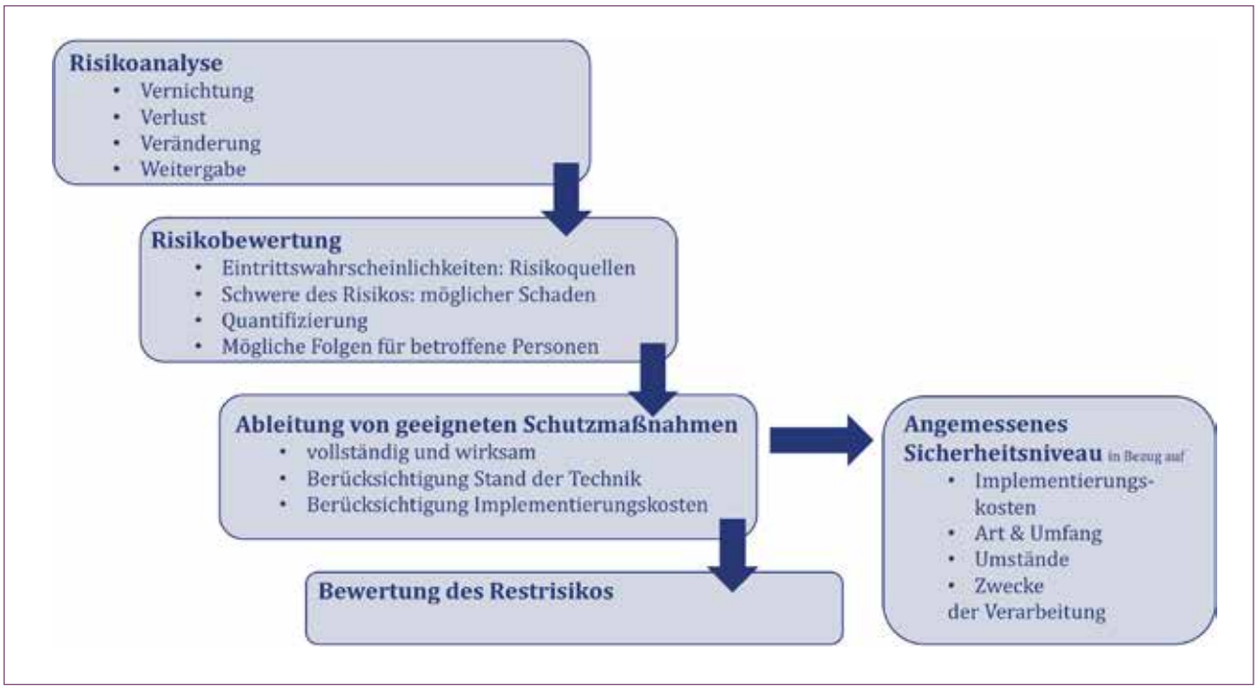



*Grafik 4: LegalThings One Hashing*
*Quelle: LegalThings One: Hashing. https://medium.com/legalthingsone/legalthings-one-blockchain-gdpr-made-possible-68a5ce09e7ca, Zugriff am 11. November 2018*

Auf die Notwendigkeit zu Erstellung einer Datenschutz-Folgenabschätzung weisen folgende objektiv und subjektiv zu bewertende Faktoren hin:

1. „Verwendung neuer Technologien" [Art. 35 Abs. 1 DSGVO],
2. „automatisierte Verarbeitung einschließlich Profiling" im Sinne einer „systematische[n] und umfassende[n] Bewertung persönlicher Aspekte" [Art. 35 Abs. 3 lit. a DSGVO], also einer gewissen Struktur oder bestimmten Prinzipien folgend,
3. „umfangreiche Verarbeitungsvorgänge ... auf regionaler, nationaler oder supranationaler Ebene" [ErwG 91 DSGVO] im Sinne von Big Data Erhebungen und Analysen,
4. „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten" [Art. 35 Abs. 3 lit. b DSGVO] im Sinne von Big Data Anwendungen, die auch, aber nicht nur in sensiblen Bereichen wie z.B. Gesundheit, Strafregister, etc. angesiedelt sind,
5. Personenanzahl,
6. „Verarbeitungsvorgänge [, bei] den[en] betroffenen Personen die Ausübung ihrer Rechte erschwer[t]" wird [ErwG 91 DSGVO],
7. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Da bei der Konzeption von Smart-Home-Produkten im Prinzip sogar alle genannten Kriterien ins Blickfeld rücken, sollten Hersteller daher „Maßnahmen, Garantien und Verfahren prüfen, mit denen Unternehmen bestehende Risiken eindämmen und die sonstigen Vorgaben der Verordnung einhalten können" [Wybitul (2017) S. 38 Rn. 118]. Speziell das Profiling, darunter fallen Angaben wie „wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, ... Aufenthaltsort oder Ortswechsel" [Wybitul (2017) S. 535, Rn. 26], kann insoweit das Risiko bergen, dass der betroffenen Person aus dem Vergleichs- und Analyseergebnis mit anderen ähnlich strukturier-




*Grafik 5: Prozesskette für die Risikoanalyse*

ten Individuen persönliche oder wirtschaftliche Nachteile entstehen, z.B. bei Versicherungsprämien oder vorenthaltenen Rabatten.

Grafik 5 veranschaulicht die Prozesskette für die Risikoanalyse im Rahmen einer Datenschutz-Folgenabschätzung.

## *Fazit*

Ausgerechnet durch die Einführung der DS-GVO wird gerade bei Unternehmen und Organisationen der Nutzen einer Installation von Smart-Home-spezifischer Komponenten deutlich. So ist im Rahmen der verpflichtend zu erstellenden oder zu aktualisierenden Datenschutz- und Sicherheitskonzepte ein ganzheitlicher Ansatz bei der Etablierung geeigneter technischer und organisatorischer Maßnahmen zu empfehlen. So ermöglichen aufeinander abgestimmte Smart-Home-Komponenten die automatisierte und annähernd wartungsfreie Überwachung aller Zutritte (durch Sicherheitsschlösser, Fenstersicherungen, Videoüberwachung), Zugänge (durch Keycards und Verschlüsselung) oder Zugriffe (durch Zwei-Faktor-Anmeldung und ein Berechtigungskonzept) in einem Unternehmensgebäude. Die Einrichtung und der Betrieb eines Smart Homes werden durch Datenschutz also nicht ausschließlich schwieriger, sondern Smart Home bietet im Gegenzug Lösungen für eine adäquate Umsetzung im Sinne des „Standes der Technik“. Um möglichst umfangreich und frühzeitig von diesen Innovationen im Smart Home- und Datenschutzbereich zu profitieren, sollten Versicherungsunternehmen zunächst eine ganzheitliche IoT-Strategie entwickeln und z.B. Kooperationen mit Herstellern und Dienstleistern in diesem Bereich ins Leben rufen. Je nach gewähltem Schwerpunkt können dann u.a. mit Hilfe von Experten für Big Data und Datenschutzfragen DSGVO-konforme Prozesse definiert und die eigenen Produkte daran weiterentwickelt werden.

Unternehmen wie die DYNACON GmbH mit Sitz in München begleiten Versicherungen und andere Unternehmen auf ihrem Weg zur Digitalisierung, indem sie mit wachsamem Auge die Innovationen auf dem Markt beobachten, sie bewerten und mit dem nötigen Know-how in maßgeschneiderte Umsetzungsstrategien transformieren.