DIN-Verbraucherrat

Studie

Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes“ Spielzeug – Umsetzung in der Normung

Impressum

Herausgeber:

DIN-Verbraucherrat
DIN e.V.

Am DIN Platz
Burggrafenstraße 6
10787 Berlin

E-Mail: verbraucherrat@din.de
Web: http://www.din.de/go/verbraucherrat

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren:

Dr. Julius Rauber und Prof. Dr. Christian Thorun

ConPolicy GmbH
Institut für Verbraucherpolitik
Crellestr. 37
10827 Berlin

www.conpolicy.de

Berlin, Dezember 2019

ConPolicy
Institut für Verbraucherpolitik

02. Dezember 2019

Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes“ Spielzeug – Umsetzung in der Normung

Ergebnisbericht für den DIN-Verbraucherrat

vorgelegt bei:
DIN e. V.
DIN-Verbraucherrat
Herrn Andreas Zause
Saatwinkler Damm 42/43
13627 Berlin

durch:
ConPolicy GmbH
Institut für Verbraucherpolitik
Crellestr. 37
10827 Berlin
www.conpolicy.de

Autoren:
Dr. Julius Rauber und Prof. Dr. Christian Thorun

Ansprechpartner:
Dr. Julius Rauber
rauber@conpolicy.de

Zusammenfassung

Anforderungen an Kinderspielzeug – insbesondere bezüglich ihrer Sicherheit – sind von besonderer Bedeutung, da Kinder als Nutzende eine besonders schutzbedürftige Verbrauchergruppe darstellen. Normen wie DIN EN 71-1 (Sicherheit von Spielzeugen) oder DIN EN 62115 (Sicherheit von elektrischen Spielzeugen) geben den Herstellern dabei klare Richtlinien zur Konstruktion der Spielzeuge vor und beschreiben, wie bestimmte Anforderungen eingehalten werden können. Zudem vermitteln sie den Käufern – im Falle von Spielzeug sind dies zumeist die Eltern – die Sicherheit, dass die Produkte gewisse Mindeststandards einhalten, wenn sie der Norm entsprechen.

Die fortschreitende Digitalisierung führt nun allerdings dazu, dass klassische, analoge Spielzeuge – wie z.B. Puppen – immer häufiger digitale Komponenten enthalten und zudem mit anderen Geräten (oder auch direkt mit dem Internet) vernetzt werden können. Dadurch können diese „smarten“ Spielzeuge neben dem „klassischen“ Produktkern – z.B. der Puppe als Gegenstand – auch Dienstleistungen – z.B., dass die Puppe auf Fragen spezifisch antwortet – anbieten. Diese Entwicklung führt dazu, dass für „smartes“ Spielzeug neue Verbraucheranforderungen (wie z.B. ein adäquater Datenschutz oder die Sicherheit von Datenverbindungen) entstehen.

Um auch in Zukunft die Sicherheit von Spielzeugen gewährleisten zu können, bedarf es also einer Analyse, wie sich die Verbraucheranforderungen an Spielzeug vor dem Hintergrund der Digitalisierung verändern und ob diese neuen Anforderungen bereits in Normen umgesetzt bzw. festgeschrieben sind.

Vor diesem Hintergrund wurde das ConPolicy-Institut für Verbraucherpolitik vom DIN Verbraucherrat damit beauftragt, **folgende Fragen** zu untersuchen:

- Welche neuen Verbraucheranforderungen entstehen durch die Digitalisierung und Vernetzung von Spielzeug?
- Inwiefern sind diese Verbraucheranforderungen schon durch bestehende Spielzeugnormen abgedeckt?
- Gibt es Normen aus anderen Bereichen, die auch für Verbraucheranforderungen an „smarte“ Spielzeuge zutreffen?
- Welche Handlungsoptionen gibt es, um die neuen Verbraucheranforderungen in Normen umzusetzen?

Für die Studie wurden mehrere **Methoden** kombiniert: Die Identifikation der Verbraucheranforderungen erfolgte weitgehend theoriebasiert und literaturgestützt. Zudem wurden die Anforderungen auch mit Expertinnen und Experten im Rahmen von Interviews auf Vollständigkeit geprüft. Danach wurden relevante Normen und Spezifikationen identifiziert, die möglicherweise Verbraucheranforderungen an

„smarte“ Spielzeuge konkretisieren könnten. Nachdem Verbraucheranforderungen mit den Normen und Spezifikationen abgeglichen wurden, diskutierten mehrere Expertinnen und Experten in einem Fachgespräch die Ergebnisse und mögliche Handlungsoptionen, um die bestehenden Lücken zu schließen.

Im Ergebnis können ***drei übergeordnete Erkenntnisse*** für die Normung von „smarten“ Spielzeugen aus Verbrauchersicht abgeleitet werden:

Zunächst existieren – **erstens** – aufgrund der Digitalisierung und Vernetzung von Spielzeugen 28 neue Verbraucheranforderungen. Die meisten der Verbraucheranforderungen betreffen dabei den Datenschutz und die Datensicherheit der „smarten“ Spielzeuge. Zudem können zwei Typen von Verbraucheranforderungen unterschieden werden: 21 Verbraucheranforderungen, die allgemein für vernetzte Geräte des „Internet of Things“ gelten und sieben Verbraucheranforderungen, die spezifisch an „smarte“ Spielzeuge zu stellen sind.

Deshalb können – **zweitens** – für „smarte“ Spielzeuge neben den einschlägigen Spielzeugnormen – wie der DIN EN 71-1 und DIN EN 62115 – auch Normen und Spezifikationen für vernetzte Geräte relevant sein. Im Rahmen der Studie wurden hier insbesondere die Spezifikationen ETSI TS 103 645 (Cyber Security for Consumer Internet of Things) und DIN SPEC 27072 (IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit) sowie die im Entwurf befindliche Norm ISO 31700 (Consumer Protection — Privacy by Design for Consumer Goods and Services) identifiziert und untersucht.

Der Abgleich von Verbraucheranforderungen und relevanten Normen und Spezifikationen zeigt – **drittens** –, dass ein heterogenes Bild bezüglich der Umsetzung von Verbraucheranforderungen für „smartes“ Spielzeug in Normen und Spezifikationen besteht: Während bei den Themen Datenschutz und Datensicherheit schon viele Aspekte in Normen oder Spezifikationen konkretisiert sind, werden andere Punkte wie die Erweiterung der Gewährleistungsrechte um Dienstleistungsaspekte oder digitale „Kindersicherungen“ noch nicht in Normen oder Spezifikationen adressiert.

Aus diesen Erkenntnissen ergeben sich **drei *Handlungsempfehlungen*** als Ansatzpunkte **für den DIN-Verbraucherrat**:

1.) **Allgemeine Verbraucheranforderungen** an vernetzte Geräte, die auch für „smarte“ Spielzeuge relevant sind, sollten entsprechend in Normen und Spezifikationen für IoT-Geräte eingebracht werden. Bezüglich des wichtigen Themas **Datensicherheit** wird deshalb u.a. eine Mitarbeit im Rahmen der neuen, europäischen Norm ETSI EN 303 645 empfohlen. Diese Norm befindet sich derzeit in der Abstimmungsphase und erfasst die wesentlichen Inhalte der Spezifikationen ETSI TS 103 645 und DIN SPEC 27072. Somit beinhaltet diese Norm schon einige wichtige Verbraucheranforderungen zur Datensicherheit, aber auch darüber hinaus.

2.) Um allgemeine Verbraucheranforderungen an das zweite wichtige Thema für vernetzte Geräte – den **Datenschutz** – in Normen umzusetzen, empfiehlt es sich,

bei der Entwicklung der internationalen Norm ISO 31700 im zuständigen Normungsausschuss ISO/PC 317 mitzuwirken. Bei dieser Norm steht das Thema Privacy by design bei vernetzten Konsumgeräten und den zugehörigen Dienstleistungen im Mittelpunkt. Von Vorteil ist hier auch das relativ frühe Entwicklungsstadium des Normungsprozesses und dass es sich um eine international gültige Norm handeln wird.

3.) **Spezifische Verbraucheranforderungen**, die ausschließlich für „smarte“ Spielzeuge gelten, sollten in der Spielzeugnormung bearbeitet bzw. Inhalte in den entsprechenden Ausschüssen eingebracht werden. Auf internationaler Ebene könnte der Ausschuss ISO/TC 181 für die **Spielzeugnormung** einen Ansatzpunkt bieten. Jedoch ist hier der Einfluss der deutschen Normung als gering einzuschätzen. Ein anderer Ansatzpunkt ist die **Norm zur Sicherheit von elektrischem Spielzeug** IEC 62115 bzw. das dafür zuständige internationale Normungsgremium IEC/TC 61. Hier müsste der Zuständigkeitsbereich der Norm und des Gremiums um elektronische und vernetzte Spielzeuge erweitert werden, damit die Bearbeitung relevanter Inhalte zu „smarten“, vernetzten Spielzeugen in diesem Gremium ermöglicht werden kann. Eine Einbringung und Umsetzung von Verbraucheranforderungen kann hier dann durchaus als chancenreich eingestuft werden.

Summary

Requirements for children's toys, in particular with regard to their safety, are of particular importance as children are a particularly vulnerable consumer group. Standards such as DIN EN 71-1 (safety of toys) or DIN EN 62115 (safety of electric toys) provide manufacturers with clear guidelines for the construction of toys and how certain requirements can be met. In addition, they give purchasers – in the case of toys these are usually the parents – the assurance that the products comply with certain minimum requirements if they comply with the standard.

As digitization progresses, classic analog toys – such as dolls – now contain digital components and can often be connected with other devices (or even directly with the Internet). This means that these "smart" toys can offer services – e.g. a doll responds specifically to questions – in addition to the "classic" product core use – e.g. playing with the doll as an object. This development leads to new consumer requirements for "smart" toys (such as adequate data protection or the security of data connections).

In order to be able to guarantee the safety of toys in the future as well, it is therefore necessary to investigate whether and to what extent consumer requirements for toys change in light of digitization and whether these new requirements have already been implemented or laid down in standards.

Against this background, the ConPolicy Institute for Consumer Policy was commissioned by DIN Consumer Council to **investigate the following questions**:

- What new consumer requirements arise from the digitization and networking of toys?
- To what extent are these consumer requirements already covered by existing toy standards?
- Are there standards from other areas that also apply to consumer requirements for "smart" toys?
- What options are there for implementing the new consumer requirements in standards?

Several **methods** were combined for the study: The identification of consumer requirements was largely based on theory and literature. In addition, the requirements were checked for completeness in interviews with experts. Relevant standards and specifications were then identified which could possibly concretize consumer requirements for "smart" toys. After consumer requirements had been compared with standards and specifications, several experts discussed the results and possible options for action in an expert discussion in order to close the existing gaps.

As a result, **three overarching findings** for the standardization of "smart" toys can be derived from the consumer's point of view:

Firstly, there are 28 new consumer requirements due to the digitization of toys. Most of the consumer requirements relate to data protection and data security of "smart" toys. In addition, two types of consumer requirements can be distinguished: 21 consumer requirements, which generally apply to networked devices of the "Internet of Things", and seven consumer requirements, which are specific to "smart" toys.

Therefore and **second**, in addition to the relevant toy standards such as DIN EN 71-1 and DIN EN 62115, standards and specifications for connected devices may also be relevant for "smart" toys. As part of the study, the specifications ETSI TS 103 645 (Cyber Security for Consumer Internet of Things) and DIN SPEC 27072 (IoT-devices – Minimum requirements for information security) as well as ISO 31700 (Consumer Protection – Privacy by Design for Consumer Goods and Services), which is currently in draft, were identified and examined.

The comparison of consumer requirements and relevant standards and specifications shows – **thirdly** – that there is a heterogeneous picture regarding the implementation of consumer requirements in standards and specifications: While many aspects of data protection and data security have already been concretized in standards or specifications, other topics such as the extension of warranty rights to include service aspects or digital "child safety lock" have not yet been addressed in standards or specifications.

These findings result in **three** different **recommendations for action** as starting points **for the DIN Consumer Council**:

1.) **General consumer requirements for connected devices** – that are also relevant for smart toys – should be included in standards and specifications for IoT devices. With regard to the important topic of **data security**, cooperation within the framework of the new European standard ETSI EN 303 645 is advised. This standard is currently in the coordination phase and covers the essential contents of the specifications ETSI TS 103 645 and DIN SPEC 27072. Thus, this standard already contains some important consumer requirements for data security, but also beyond that.

2.) In order to implement general consumer requirements on the second important topic for connected devices – **data protection** – in standards, it is advisable to participate in the development of the international standard ISO 31700 in the ISO/PC 317 standards committee. This standard focuses on privacy by design for connected consumer devices and related services. Another advantage here is the relatively early development stage of the standardization process and the fact that it will be an internationally valid standard.

3.) **Specific consumer requirements** for "smart" toys should be dealt with in **toy standardization** or content should be introduced in the relevant committees. At the international level, the ISO/TC 181 committee could provide a starting point for toy standardization. However, the influence of German standardization is to be assessed as low here. Another entry point is the IEC 62115 standard on the **safety**

of electrical toys and the IEC/TC 61 international standardization body responsible for it. Here, the scope of the standard and the committee would have to be extended to include electronic and connected toys. The introduction and implementation of consumer requirements for “smart” toys can then certainly be classified as promising.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Durch die Digitalisierung ist eine neue Gruppe von Spielzeugen entstanden: Sogenannte „smarte“ Spielzeuge können mit den Kindern beim Spielen interagieren, etwa indem sie Kindern Fragen beantworten oder auf deren Bewegungen entsprechend reagieren.[1] Dazu greifen die Spielzeuge auf integrierte Prozessoren zurück oder sind mit dem Internet verbunden. Neben den neuen Nutzungsmöglichkeiten für die Kinder und Eltern entstehen durch diese Entwicklung auch neue Verbraucheranforderungen. So müssen „smarte“ Spielzeuge nun nicht mehr allein physischen Sicherheitsanforderungen entsprechen (z.B., dass Spielzeuge für Kleinkinder unter 36 Monaten keine verschluckbaren Kleinteile enthalten dürfen), sondern auch Anforderungen bezüglich neuer Dimensionen wie Datenschutz oder Datensicherheit erfüllen. Entsprechende Verbraucheranforderungen werden inzwischen auch von verschiedenen Stakeholdern wie Verbraucherschutzorganisationen, Prüfinstitutionen oder politischen Parteien erhoben. So hat z.B. die niederländische Radiocommunications Agency eine Studie zum Stand der Sicherheit von IoT-Geräten beauftragt, die sich unter anderem auch mit „smarten“ Spielzeugen beschäftigt. In der Studie werden „smarte“ Spielzeuge anhand bestimmter Kriterien – wie etwa privacy und security by design bzw. default – untersucht und bewertet, inwiefern sie Verbraucheranforderungen erfüllen.[2]

Solche Verbraucheranforderungen werden zudem häufig in Normen konkretisiert und festgeschrieben. Im Normungsprozess einigen sich verschiedene gesellschaftliche Gruppen auf bestimme Mindeststandards, die bei Befolgung der Norm durch die Hersteller eingehalten werden. Insbesondere bei Produkten für schutzbedürftige Verbrauchergruppen – wie Kinder als Nutzer von Spielzeugen – sind sie von besonderer Bedeutung. Da „smarte“ Spielzeuge noch eine vergleichsweise neue Erscheinung darstellen und Normungsprozesse häufig über Jahre angelegt sind, dürften viele neue Verbraucheranforderungen an „smarte“ Spielzeuge noch nicht in Normen niedergeschrieben sein.

Ausgehend von diesen Erkenntnissen wurde das ConPolicy-Institut für Verbraucherpolitik vom DIN-Verbraucherrat (DIN-VR) mit der Erstellung der vorliegenden Studie beauftragt. Dabei stellen die Identifikation und Kondensierung der wichtigsten Verbraucheranforderungen an „smarte“ Spielzeuge einen Fokus dieser Studie dar. Ein weiterer Schwerpunkt der Studie liegt auf dem Abgleich der Verbraucheranforderungen mit bestehenden Normen und dem Herausarbeiten von entsprechenden Lücken. Darüber hinaus sollen konkrete Handlungsempfehlungen dazu entwickelt werden, wie der DIN-VR in seiner Normungsarbeit für eine Umsetzung der Verbraucheranforderungen in Normen sorgen kann.

---

[1] Roth, A., & Möslein, K. M. (2014). Produzenten als Dienstleister: Auf dem Weg zu interaktiven hybriden Wertschöpfungssystemen. In Enterprise-Integration (pp. 139-151). Springer Vieweg, Berlin, Heidelberg.
[2] Strict B.V. (2019). Report on IoT Device Security. Abgerufen von: https://www.agentschaptele-com.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur (21.10.2019).

Der Bericht ist wie folgt aufgebaut: In Kapitel 2 wird zunächst „smartes“ Spielzeug definiert und es werden Kategorisierungen für „smarte“ Spielzeuge erläutert. Nach dieser Einführung werden in Kapitel 3 anhand der Ergebnisse einer umfassenden Literaturrecherche und mit Hilfe von Experteninterviews 28 Verbraucheranforderungen vorgestellt, die an „smarte“ Spielzeuge gestellt werden sollten bzw. müssen. Im vierten Kapitel wird erläutert, inwiefern diese Verbraucheranforderungen schon in bestehenden Normen bzw. Spezifikationen adressiert werden. Der Bericht schließt in Kapitel 5 mit Empfehlungen für Handlungsstrategien.

1.1. Zielsetzung und Fragestellungen

Der DIN-VR verfolgt mit der Studie **zwei übergeordnete Ziele**: Zum einen soll der **gegenwärtige Stand** bei der Umsetzung neuer Verbraucheranforderungen in der Normung bzw. in bestehenden Spielzeugnormen wie der DIN EN 71-1 „Sicherheit von Spielzeug - Mechanische und physikalische Eigenschaften“ oder der DIN EN 62115 „Elektrische Spielzeuge - Sicherheit“ betrachtet und bestehende Lücken benannt werden. Das zweite Ziel besteht darin, Handlungsfelder für das Schließen dieser Lücken zu erkennen und mögliche **Handlungsoptionen** zu beschreiben. Dazu sollen im Rahmen der Studie folgende Fragestellungen adressiert werden:

Ziel 1: Erforschung des Status Quo der Normung von „smarten“ Spielzeugen

1) Identifikation von Verbraucheranforderungen an „smarte“ Spielzeuge

- Welche neuen Verbraucheranforderungen entstehen vor dem Hintergrund digitaler Entwicklungen? In welchen Bereichen, d.h. für welche Leitwerte des DIN-VR, entstehen diese Anforderungen? Gelten diese Verbraucheranforderungen nur für „smarte“ Spielzeuge oder auch für andere vernetzte Geräte?

2) Stand der Umsetzung neuer Verbraucheranforderungen an „smarte“ Spielzeuge in Normen

- Welche Normen und Spezifikationen sind für „smarte“ Spielzeuge relevant? Handelt es sich dabei um Spielzeugnormen oder Normen, die andere Bereiche wie z.B. vernetzte Geräte allgemein betreffen?
- Welche Verbraucheranforderungen werden schon in Normen konkretisiert? Welche Lücken bestehen derzeit noch?

Ziel 2: Bestimmung und Beschreibung möglicher Handlungsoptionen

1) Identifikation von möglichen Handlungsoptionen

- Betreffen die bestehenden Lücken eher allgemeine oder Spielzeug-spezifische Verbraucheranforderungen? In welchen Normungsfeldern können diese Verbraucheranforderungen jeweils adressiert werden? Bedarf es einer Konkretisierung bestehender Spielzeugnormen, der Überarbeitung von

Querschnittsnormen oder einer Entwicklung neuer Normen? Wer sind die zuständigen Personen oder Gremien hierfür?

2) Entwicklung von Handlungsempfehlungen

- Wie sollte der DIN-VR konkret vorgehen? Welche aktuellen Normungsvorhaben gibt es? Inwiefern können hier verschiedene Ideen und Vorschläge eingebracht werden?

1.2. Methodik

Das Vorhaben wurde in vier Arbeitspaketen (AP) (vgl. Abbildung 1) unter Anwendung der folgenden Methodik umgesetzt:

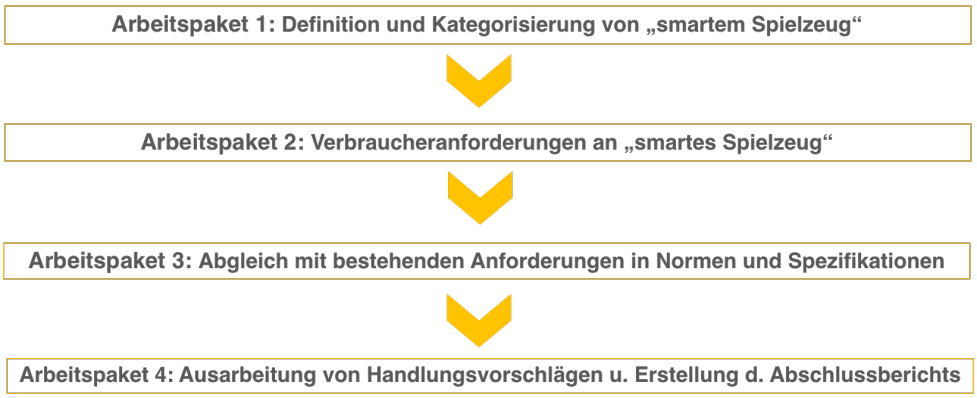

Abbildung 1: Darstellung der Arbeitspakete

Die Erarbeitung der konzeptionellen Grundlagen in Form einer **Definition und Kategorisierung von „smartem“ Spielzeug in AP 1** (Kapitel 2.1 und 2.2) fällt in den Bereich der analytischen Forschung und erfolgte theoriebasiert und literaturgestützt. Dieser Schritt diente vor allem dazu, dass der Forschungsgegenstand – also wie „smarte“ Spielzeugen im Rahmen dieser Studie abgegrenzt werden – klar bestimmt ist.

Zur Ableitung der **Verbraucheranforderungen an „smartes Spielzeug“ in AP 2** (Kapitel 3) wurden mehrere Schritte kombiniert: Zunächst wurde der Einfluss der Digitalisierung auf die **acht Leitwerte des DIN-VR** betrachtet und untersucht, inwiefern diese Leitwerte für die Bestimmung von neuen Verbraucheranforderungen als Ausgangspunkt dienen können (3.1). Im nächsten Schritt wurden dann im Rahmen einer umfassenden Literaturrecherche sowie durch Gespräche mit Expertinnen und Experten **neue Verbraucheranforderungen**, die durch die Digitalisierung und Vernetzung von Spielzeugen entstanden sind, für die einzelnen Leitwerte identifiziert und erläutert (3.2.1 – 3.2.8). Abschließend wurden diese Verbraucheranforderungen in allgemeine sowie Spielzeug-spezifische Anforderungen eingeteilt und in einer Übersichtstabelle aufgelistet (3.2.9)

In **AP 3** wurden dann bestehende, relevante **Normen und Spezifikationen** identifiziert und mit den Verbraucheranforderungen abgeglichen. Auch hier wurden mehrere Methoden genutzt: Zunächst wurden alle Normen und Spezifikationen herausgesucht, die „smarte“ Spielzeuge betreffen könnten (4.1). Diese Normen und Spezifikationen wurden durch eine Recherche in Normendatenbanken, die Betrachtung anstehender Normungsvorhaben, Gesprächen mit der Geschäftsstelle des DIN-VR und den Experten identifiziert. Diese Normen und Spezifikationen wurden dann auf Inhalte untersucht, die den Verbraucheranforderungen aus Kapitel 3.2 entsprechen. Das Ergebnis der Untersuchung wurde im Rahmen eines Fachgesprächs mit Expertinnen und Experten diskutiert und die neuen Erkenntnisse flossen in Kapitel 4.2 dieses Berichts entsprechend ein. Das Ergebnis dieses Arbeitspakets wird abschließend in einer Übersichtstabelle schematisch dargestellt.

In **AP 4** (Kapitel 5) werden Handlungsvorschläge vorgestellt, wie die identifizierten Lücken zwischen Verbraucheranforderungen und bestehenden Normen geschlossen werden können. Die Vorschläge basieren auf den Erkenntnissen der Studie und wurden ebenfalls im Fachgespräch mit den Experten diskutiert und weiterentwickelt. Abschließend wurden sie in einem Abschlussgespräch nochmals präsentiert sowie geprüft, bevor sie in den Bericht einflossen.

2. Definition und Kategorien von „smartem“ Spielzeug

2.1. Definition des Begriffs „smartes“ Spielzeug

Unter Spielzeug im Allgemeinen versteht man ein Produkt, „das, ob ausschließlich oder nicht, zum Spielen für Kinder unter 14 Jahren konzipiert oder eindeutig dafür bestimmt ist.“[3] Unter „Spielen“ wurden dabei bisher ausschließlich Handlungen des Kindes mit dem Spielzeug verstanden, d.h. dem Spielzeug selbst kam dabei eine passive Rolle zu.

„Smarte“ Spielzeuge (oder auch „intelligente“ Spielzeuge oder „smart toys“) können hingegen auch auf Handlungen, Verhaltensweisen oder Sprachbefehle der Nutzer eingehen.[4] Dazu werden zumeist entweder integrierte Sensoren, Kameras oder Mikrofone eingesetzt, wodurch Daten über das Verhalten oder Aussagen der Kinder aufgezeichnet und verarbeitet werden können.[5] Die Spielzeuge können dann „intelligent“ auf die Handlungen bzw. Aussagen der Kinder reagieren. Das Spielzeug „Dino“ antwortet beispielsweise auf die Frage nach der Entfernung des Mondes dem Alter des Kindes entsprechend. Ein fünfjähriges Kind bekommt deshalb die Antwort „Es ist sehr weit. Zu weit zum Laufen“, während ein neunjähriges Kind „Der Mond ist 238.900 Meilen weg und bewegt sich jedes Jahr weiter weg“ als Antwort erhält.[6]

Im Rahmen dieser Studie werden unter „smarten“ Spielzeugen ausschließlich Spielzeuge verstanden, die – vernetzt oder unvernetzt – intelligent und spielerisch mit den Kindern interagieren.[7] Originär für die Kinderüberwachung genutzte Produkte wie Babyassistenzsysteme zählen hier nicht zu „smarten“ Spielzeugen, da bei diesen nicht der spielerische Aspekt im Vordergrund steht.[8]

---

[3] DIN EN 62115: Elektrische Spielzeuge – Sicherheit

[4] Bundesamt für Sicherheit in der Informationstechnik (o.D.). Smartes Spielzeug – Lernhilfen oder Spion? Abgerufen von: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html (21.10.2019).

[5] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

[6] Internet Innovators (2017). Smart Toys und Connected Smart Toys: Hell No Barbie. Abgerufen von: https://internetinnovators.com/de/post-de/hell-no-barbie/ (21.10.2019).

[7] Weitere Informationen zu „smarten“ Spielzeugen und Beispiele sind im Faktenblatt „Smartes Spielzeug: Produktübersicht, Funktionen, Verbreitung, Vor- und Nachteile für Verbraucher sowie verbraucherpolitische Konsequenzen“ zu finden. Abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Berichte/Faktenblatt_Smartes-Spielzeug.pdf?__blob=publicationFile&v=1 (21.10.2019).

[8] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

2.2. Kategorien von „smarten“ Spielzeugen

„Smarte“ Spielzeuge können nach verschiedenen Kategorien geordnet werden. Für eine Kategorisierung nach der **Art der Vernetzung** ist der Ort der Datenverarbeitung von grundlegender Bedeutung. Während einige Spielzeuge durch einen integrierten Prozessor die Daten direkt lokal verarbeiten können, kommunizieren andere Spielzeuge dafür mit mobilen Endgeräten durch Apps oder aber direkt mit externen Servern über das Internet. Folglich kann bezüglich der **Vernetzung** zwischen **drei Gruppen** unterschieden werden:

Unvernetzte „smarte“ Spielzeuge, die durch die eingebaute Sensorik selbstständig und autark reagieren können. Diese Spielzeuge haben keine Verbindung zu externen Servern oder Geräten über das Internet. Die Turtles-Puppe Talk-to-me-Mikey kann beispielsweise durch einen eingebauten Prozessor auf Fragen von Kindern antworten. Zudem beinhaltet sie einen elektronischen Sensor, durch welchen sie auch Bewegungen registrieren und auf diese mit entsprechenden Kommentaren reagieren kann.

Neben diesen unvernetzten Spielzeugen gibt es zwei Arten von **vernetzten Spielzeugen** (sogenannte „connected smart toys“): Einerseits gibt es Spielzeuge, die über **Schnittstellen** (wie z.B. Bluetooth) **mit anderen mobilen Endgeräten** wie Smartphones oder Tablets in der näheren Umgebung kommunizieren können. Über diese Endgeräte können die Nutzer das Spielzeug per App steuern. Zudem kann häufig über diese Endgeräte auch eine Verbindung mit externen Servern und dem Internet hergestellt werden. Beispielhaft hierfür sind die Puppe Dino oder der Roboter-Hund Chip.[9]

Außerdem gibt es Spielzeuge, die über eine integrierte **IP-Schnittstelle über das WLAN direkt mit externen Servern bzw. dem Internet** verbunden werden können. Ein Beispiel hierfür ist die Puppe Hello Barbie. Sie verfügt über ein Mikrofon und übermittelt per WLAN aufgezeichnete Sprachdateien direkt an einen externen Server. Hier werden diese verarbeitet und eine adäquate Antwort wird zurückgesendet und dem Kind über die Puppe ausgegeben.[10]

Neben dieser grundlegenden, technischen Unterscheidung zwischen vernetzten und unvernetzten Spielzeugen gibt es auch **weitere Kategorisierungsarten**, die andere Aspekte berücksichtigen. So differenzieren beispielsweise die Marktwächter der Verbraucherzentralen nach der optischen Erscheinung sowie der Kernfunktionen eines „smarten“ Spielzeugs.[11] In ihrem Bericht unterscheiden sie zwischen

[9] Future of Privacy Forum (2016): Kids and the connected home: Privacy in the age of connected dolls, talking dinosaurs, and battling robots. Abgerufen von: https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf (20.10.2019).

[10] Internet Innovators (2017). Smart Toys und Connected Smart Toys: Hell No Barbie. Abgerufen von: https://internetinnovators.com/de/post-de/hell-no-barbie/ (21.10.2019).

[11] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

- Figuren mit Spracherkennung zur Kommunikation mit dem Kind (wie z.B. Hello Barbie),
- ferngesteuerten Spielzeugen, die über mobile Endgeräte per App gesteuert werden können (z.B. Spielzeugautos oder Drohnen),
- Spielzeugrobotern, die Gegenstände transportieren oder Stapeln können (z.B. Sphero 2.0) und
- interaktiven Lernspielzeugen, die als Kernziel die Förderung der kognitiven Fähigkeit des Kindes haben (z.B. speziell für Kinder entwickelte Tablets).

Ein Dokument der von der EU finanzierten Initiative BEESECURE[12] unterscheidet weiterhin zwischen

- virtuellen Freunden
- kommunizierenden Smart-Toys
- Smart-Toys mit Überwachungsfunktionen
- Drohnen
- sozialen Smart-Toys
- entwicklungsfähigen Smart-Toys
- Virtual Reality
- pädagogischen Smart-Toys

Diese Kategorisierungen bieten jedoch einerseits nur bedingt eine Hilfestellung, um Verbraucheranforderungen für „smarte“ Spielzeuge zu identifizieren bzw. zu differenzieren (wie etwa Unterscheidungen nach optischen Erscheinungen) und umfassen andererseits Geräte, die nicht mehr unter die hier genannte Definition von „smarten“ Spielzeugen fallen (wie etwa Smart-Toys mit Überwachungsfunktionen oder Drohnen). Deshalb wird im Rahmen dieser Studie vor allem auf die Unterscheidung nach verschiedenen Formen der Vernetzbarkeit zurückgegriffen und die Verbraucheranforderungen dementsprechend formuliert.

[12] Bee Secure (2010-2019). Smart Toys. Abgerufen von: https://www.bee-secure.lu/de/themen/internet-of-things/smart-toys (20.10.2019).

3. Verbraucheranforderungen an „smartes“ Spielzeug

3.1. Neue Verbraucheranforderungen durch die Digitalisierung und Auswirkungen auf die DIN-VR Leitwerte

Im Zuge der Digitalisierung entwickeln sich die Anforderungen von Verbraucherinnen und Verbrauchern an Produkte und Dienstleistungen weiter. Dies wirkt sich auch auf den Normungsprozess und die daraus resultierenden Normen aus. Das verdeutlicht etwa die Studie „Strategisches Konzept zum Umgang mit der Digitalisierung“ von ConPolicy im Auftrag des DIN-Verbraucherrats (2018).[13] Die Studie kommt zu dem Schluss, dass die bestehenden Leitwerte des DIN-VR auch in Zukunft grundsätzlich den Kompass für eine adäquate Vertretung der Verbraucherinteressen in der Normung bilden können. Diese Leitwerte sind:

1. Sicherheit und gesundheitliche Unversehrtheit der Verbraucher
2. Datenschutz und Datensicherheit, sowie Schutz der Persönlichkeitsrechte
3. Verhindern ökonomischer Nachteile für Verbraucher
4. Gebrauchstauglichkeit und Qualität von Produkten und Dienstleistungen
5. Prinzipien der Nachhaltigkeit (gleichwertige Berücksichtigung ökonomischer, ökologischer und sozialer Aspekte)
6. Herstellung von Transparenz und Vergleichbarkeit auf Märkten
7. Schutz vor Täuschung
8. Interessen besonders schutzbedürftiger gesellschaftlicher Gruppen

Für die **Normungsarbeit** und die Leitwerte ergeben sich laut der Studie allerdings **drei grundsätzliche** – aus der **Digitalisierung** entstehende – **Herausforderungen**:

- Die Grenzen zwischen Produkten und Dienstleistungen verschwimmen im Zuge der Digitalisierung und es entstehen zunehmend „hybride“ Produkte mit Dienstleistungskomponenten. Dies führt zu einer Verschiebung der Normungsgegenstände.
- Spezifische Bereiche der Normung müssen angepasst und erweitert werden. So muss etwa bei vernetzten Produkten neben der klassischen Produktqualität auch auf Fragen der informationellen Selbstbestimmung eingegangen werden.
- Die Inhalte der jeweiligen Leitwerte müssen angepasst und ggf. erweitert werden, um den zusätzlichen Herausforderungen der Digitalisierung gerecht zu werden. Dies betrifft beispielsweise den zunehmenden Einsatz

[13] ConPolicy (2018): Entwicklung eines strategischen Konzepts zum Umgang mit der Digitalisierung in der Normung im Auftrag des DIN-Verbraucherrats.

von elektrischen und elektronischen Bauteilen, wodurch es einer Erweiterung des Sicherheitsbegriffs um den Schutz vor elektromagnetischer Strahlung oder die Kontrolle über Schnittstellen vernetzter Geräte bedarf.

Diese **Erkenntnisse gelten** insbesondere **für „smarte“ Spielzeuge**, denn bei diesen

- steht die nutzergerechte, intelligente Reaktion der Spielzeuge auf Handlungen des Kindes – zumeist durch Nutzung einer Cloud – im Fokus. Deshalb müssen Backend-Services, die in der Cloud erbracht werden, mitberücksichtigt werden.
- müssen zusätzliche Anwendungen zur Steuerung der Produkte – wie etwa Smartphone-Apps – in die Betrachtung miteinbezogen werden.
- sind personenbezogene Daten von großer Bedeutung und somit wird die Wahrung der informationellen Selbstbestimmung – auch durch die Eltern – immer wichtiger.
- müssen die Digital-Kompetenzen unterschiedlicher Verbrauchergruppen berücksichtigt werden. Diese Kompetenzen hängen dabei immer spezifischer vom Normungsobjekt ab: Bei Spielzeugen für Kleinkinder übersteigt beispielsweise die Kompetenz der Eltern die der Kinder. Bei Spielzeug für ältere Kinder kann dies umgekehrt sein.

Damit die Leitwerte des DIN-VR weiterhin die Grundlage für eine adäquate Vertretung der Verbraucherinteressen in der Normungsarbeit bilden, sollten ihre Inhalte um die Herausforderungen der Digitalisierung demnach erweitert werden. Deshalb dienen die Leitwerte im Folgenden als Ausgangspunkt für die Recherche nach neuen Verbraucheranforderungen an „smartes“ Spielzeug, deren Ergebnisse im nächsten Kapitel vorgestellt werden.

3.2. Verbraucheranforderungen für „smartes“ Spielzeug

Verbraucheranforderungen an „smartes“ Spielzeug sind von großer Bedeutung, da Kinder als Nutzerinnen und Nutzer eine besonders schutzbedürftige gesellschaftliche Gruppe darstellen. Dass solche Anforderungen noch viel mehr von den Herstellern berücksichtigt werden müssen, verdeutlicht ein Zitat von Amanda Long, der ehemaligen Direktorin von Consumers International: *"Kinder sollten nicht mit einem potenziellen Spion in ihren Schlafzimmern aufwachsen und Eltern sollten sich keine Sorgen darüber machen müssen, wer zuhört. […] Wir brauchen Hersteller, die sich zu Beginn des Designprozesses mit Sicherheit und Datenschutz befassen und nicht um Vergebung bitten, wenn ein weiterer Sicherheitsfehler in den Schlagzeilen steht."*[14]

[14] Consumers International (2018). ‘Huggybug your family today‘: Don’t play with your children’s online safety. Abgerufen von: https://www.consumersinternational.org/news-resources/news/releases/huggybug-your-family-today/ (20.10.2019) (Zitat nach eigener Übersetzung).

Neben Sicherheit und Datenschutz gibt es jedoch noch weitere Anforderungen, die aus Verbrauchersicht an „smartes“ Spielzeug gestellt werden sollten. Dazu zählen unter anderem die vorvertragliche Transparenz vor dem Kauf über bestimmte Vertragsbedingungen oder die Sicherstellung der dauerhaften Gebrauchstauglichkeit des Spielzeugs.

Solche Verbraucheranforderungen finden sich in gesetzlichen Regelungen, Prüfkriterien von Institutionen (wie dem TÜV), Positionspapieren von Verbänden (wie von Verbraucherorganisationen), Veröffentlichungen aus der Verbraucherforschung oder Institutionen (wie der Verbraucherschutzministerkonferenz) wieder.

Deshalb wurden solche Quellen identifiziert und auf mögliche Verbraucheranforderungen für „smarte“ Spielzeuge untersucht. Folgende Dokumentarten wurden im Rahmen der Recherche untersucht:

- Anforderungen in Gesetzestexten wie z.B. in europäischen Richtlinien und Verordnungen oder Gesetzen auf nationaler Ebene
- Verordnungen und Richtlinien von zuständigen Behörden wie z.B. dem Bundesamt für Sicherheit in der Informationstechnik oder der Bundesnetzagentur
- Forderungen von Interessensvertretern wie z.B. dem Verbraucherzentrale Bundesverband (vzbv), der Europäischen Vereinigung zur Koordinierung der Vertretung der Verbraucher in der Normung (ANEC) oder Consumers International (CI)
- Forderungen von politischen Akteuren wie z.B. der Verbraucherschutzministerkonferenz und Parteien
- Kriterien von prüfenden Institutionen wie z.B. dem TÜV oder der Stiftung Warentest

Dabei wurde folgendermaßen vorgegangen: Zunächst wurden Anforderungen aus Sicht von Verbraucherinnen und Verbrauchern identifiziert, die sich spezifisch auf „smarte“ Spielzeuge beziehen. Da das Feld der „smarten“ Spielzeuge noch recht jung und die Anzahl der bereits formulierten Verbraucheranforderungen begrenzt ist, wurden zudem Verbraucheranforderungen ermittelt, die sich auf vernetzte Geräte des Internet of Things im Allgemeinen beziehen. Diese Verbraucheranforderungen treffen häufig auch auf „smarte“ Spielzeuge zu, wenn diese vernetzte Spielzeuge sind und somit zum Internet of Things zählen.

Nach der Literaturrecherche wurden zusätzlich Interviews mit Expertinnen und Experten[15] zum Thema „smartes“ Spielzeug geführt. Dadurch sollen auch aktuelle Entwicklungen und Standpunkte, die noch nicht in veröffentlichten Positionspapieren artikuliert wurden, erfasst und deren Ergebnisse in die Entwicklung der Verbraucheranforderungen eingebracht werden.

[15] Interviews wurden mit Vertretern der Marktwächter, des TÜV Rheinland, des TÜV Süd, der Bundesnetzagentur, der Stiftung Warentest und mit Experten aus Normungsgremien geführt.

Die so identifizierten Verbraucheranforderungen werden im Folgenden für jeden der acht Leitwerte des DIN-VR vorgestellt.

3.2.1. Leitwert 1: Sicherheit und gesundheitliche Unversehrtheit der Verbraucher

Bei diesem Leitwert ging es ursprünglich typischerweise um Fragen zu Inhaltsstoffen von Spielzeug, die Gefahr des Verschluckens von Kleinteilen oder das Vermeiden von Quetsch- und Scherstellen.

Für „smarte“ Spielzeuge gibt es zudem weitere Risiken für die gesundheitliche Unversehrtheit. So werden „smarte“ Spielzeuge im Gegensatz zu herkömmlichen Spielzeugen, die nicht elektrisch oder elektronisch betrieben wurden, mit Strom betrieben. Deshalb ist eine elektrische Sicherheitsprüfung etwa im Hinblick auf den Schutz vor einem elektrischen Schlag wichtig. Zudem senden solche Spielzeuge auch elektromagnetische Strahlungen aus, die von der Weltgesundheitsorganisation als „möglicherweise krebserregend“ eingestuft werden.[16] Da „smarte“ Spielzeuge wie Roboter sich häufig auch bewegen, können Unfälle passieren, die mit herkömmlichem Spielzeug nicht denkbar waren. Solche Situationen sind bisher nicht geregelt und entsprechende Richtlinien für Maschinen schließen Spielzeug aus.[17] Auch gibt es Warnungen, dass die körperliche Entwicklung eingeschränkt bzw. behindert werden kann. So verfügen manche Spielzeuge über Bildschirme, deren häufige Nutzung durch das Kind zu Sehstörungen führen können.[18] Zudem fordert die Richtlinie zur Sicherheit von Spielzeugen der EU, dass „strengere und umfassendere Normen zur Begrenzung der Höchstwerte der […] Impulsgeräusche und Dauergeräusche festgelegt werden“ müssen, was insbesondere für „smarte“ Spielzeuge relevant ist.[19]

Die Marktwächter (2018) geben überdies zu bedenken, dass vernetzte Spielzeuge über Schnittstellen drahtlos kommunizieren (wie etwa über WLAN, Bluetooth etc.) und somit unerlaubt fremdgesteuert und zu Angriffen auf Kinder genutzt werden könnten.[20] Diese können dabei physischer (das Spielzeug attackiert das Kind) oder psychischer (über die Sprachausgabe wird mit dem Kind in unangemessener Form kommuniziert) Natur sein. Zudem könnten über eine unerlaubte Kontaktaufnahme Kinder zum Öffnen der Tür oder dem Verlassen des Hauses bewegt werden, was die Täter für körperliche Übergriffe nutzen könnten.

Aus dieser Diskussion lassen sich zwei Verbraucheranforderungen (VA) für den ersten Leitwert ableiten:

---

[16] Securitymadein.lu (o.D.). Smart Toys, Multiple Facetten, Multiple Risiken. Abgerufen von: https://www.bee-secure.lu/sites/default/files/publications/Article_Jouets_connectes-DE_UA.pdf (21.10.2019).

[17] Anmerkungen einer Expertin bzw. eines Experten im Interview.

[18] Securitymadein.lu (o.D.). Smart Toys, Multiple Facetten, Multiple Risiken. Abgerufen von: https://www.bee-secure.lu/sites/default/files/publications/Article_Jouets_connectes-DE_UA.pdf (21.10.2019).

[19] Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates über die Sicherheit von Spielzeug (2009). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009L0048&from=DE (20.10.2019).

[20] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

VA1: Von „smarten“ Spielzeugen dürfen keine Gefahren durch elektrische Schläge, elektromagnetische Strahlung oder selbständigen Bewegungen des Spielzeugs ausgehen. Zudem dürfen durch Bildschirme keine Sehstörungen bei Kindern entstehen und es bedarf Höchstwerten bezüglich der Geräuschbelastung.

VA2: Eine unbefugte Kontaktaufnahme durch Dritte und Manipulation der Kinder über einen unerlaubten Fernzugriff, die zu einer physischen oder psychischen Schädigung führen kann, muss ausgeschlossen sein.

3.2.2. Leitwert 2: Datenschutz und Datensicherheit, sowie Schutz der Persönlichkeitsrechte

Bei diesem Leitwert werden die Auswirkungen der Digitalisierung auf Produkte und Dienstleistungen am sichtbarsten. Daher gibt es diesbezüglich auch eine Vielzahl von Verbraucheranforderungen an „smarte“ Spielzeuge. Hierbei gilt es insbesondere, das Grundrecht auf informationelle Selbstbestimmung für die Kinder als Nutzerinnen und Nutzer der „smarten“ Spielzeuge sowie den Jugendschutz zu gewährleisten. Auch muss hier klar die Rolle der Eltern als Erziehungsberechtigte berücksichtigt werden.

Grundsätzlich ist bei diesem Leitwert auf die enge Beziehung von Datenschutz und Datensicherheit hinzuweisen. Der beste Datenschutz läuft ins Leere, wenn die Datensicherheit nicht gewährleistet ist. Auch kann die beste Datensicherheit die Privatsphäre der Verbraucher nicht schützen, wenn Datenschutzanforderungen nicht ausreichend berücksichtigt werden.[21]

Der **Datenschutz** stellt demnach das erste Standbein dieses Leitwerts dar. Seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 gilt es, deren Anforderungen konsequent in der Normung zu berücksichtigen und unbestimmte Rechtsbegriffe verbraucherfreundlich auszulegen und untergesetzlich zu konkretisieren. Bei „smarten“ Spielzeugen sind hierbei vor allem der besondere Schutz von Kindern sowie die Trennung zwischen den Nutzerinnen und Nutzern – den Kindern – und ihren Erziehungsberechtigten zu berücksichtigen.

Der effektivste Schutz der informationellen Selbstbestimmung besteht darin, dass Daten erst gar nicht erhoben werden. Daher ist bei vernetzten Spielzeugen dafür Sorge zu tragen, dass diese über leicht zugängliche Einstellungsmöglichkeiten verfügen, um die Vernetzung eines Geräts vollständig auszuschalten, um dem

[21] Organisation for Economic Co-operation and Development (OECD)(2013). Guidelines on the protection of privacy and transborder flows of personal data. Abgerufen von: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflows ofpersonaldata.htm (20.10.2019) und
United Nations Conference on Trade and Development (UNCTAD) (2016). Data protection regulations and international data flows: Implications for trade and development. Abgerufen von: https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (20.10.2019).

„Recht auf nicht-Vernetzung“ zu entsprechen.[22] Dies gilt für die Verbindungen zwischen Spielzeug und der App des Steuerungsgeräts (zumeist eine Bluetooth-Verbindung) und insbesondere auch für direkte (vom Spielzeug ausgehende) und indirekte (vom Steuerungsgerät ausgehende) Verbindungen zum Internet, da hier Daten an externe Server übertragen werden.

Zudem dürfen die erhobenen Daten nur für die dafür vorgesehenen Zwecke verarbeitetet werden. Sofern ein „smartes“ Spielzeug personenbezogene Daten verarbeitet, müssen die Hersteller nach der DSGVO dafür Sorge tragen, dass die Produkte so ausgestaltet sind, dass möglichst wenige personenbezogene Daten verarbeitet werden und Einstellungsmöglichkeiten zum Privatsphäreschutz möglichst einfach und intuitiv zu handhaben sind (Privacy by design).[23] Auch sollten die Grundeinstellungen so voreingestellt sein, dass möglichst wenig personenbezogene Daten verarbeitet werden (Privacy by default).[24] Dazu gehört unter anderem, dass Daten grundsätzlich lokal auf dem Spielzeug gespeichert werden oder der Zugriff auf Standortdaten standardmäßig ausgeschaltet ist.[25]

Falls ein „smartes“ Spielzeug eine Datenverarbeitung nicht auf eine rechtliche Erlaubnisnorm stützen kann (vgl. Art. 6 DSGVO), ist eine Einwilligung erforderlich.[26] Bei minderjährigen Kindern bis 16 Jahren ist hierfür eine Zustimmung des Erziehungsberechtigten notwendig (vgl. Art. 8 DSGVO). Deshalb müssen die Eltern als Erziehungsberechtigte bei der Erstinbetriebnahme eines „smarten“ Spielzeugs sowie bei Updates und sonstigen Veränderungen ausdrücklich nach ihrer Einwilligung zu verschiedenen Aspekten der Datenübertragung gefragt werden. Eine übersichtliche, verständliche, leicht zugängliche und gleichzeitig umfassende Darstellung der Datenschutzrichtlinien ist dazu notwendig (vgl. Art. 7 DSGVO). Wie in der DSGVO verlangt sollte Verbraucherinnen und Verbrauchern überdies die Möglichkeit gegeben werden, differenziert in die Verarbeitung ihrer Daten einzuwilligen und eine Einwilligung muss freiwillig und widerrufbar sein. Um die Freiwilligkeit zu

---

[22] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

[23] Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

[24] Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

[25] Verbraucherschutz-Minister Konferenz (24.05.2019). Top 17: Smart Toys – Daten- und verbraucherschützende Vorkehrungen für besonders schutzwürdige Verbraucher(innen) treffen Abgerufen von: https://www.verbraucherschutzministerkonferenz.de/documents/ergebnisprotokoll-der-15-vsmk-am-24052019-in-mainz_rlp-extern_1559902425.pdf (21.10.2019) und
Verbraucherzentrale Bundesverband e.V. (2017). Hintergrundpapier des VZBV zum Thema Smart Home. Abgerufen von: https://www.vzbv.de/sites/default/files/downloads/2017/09/05/170905_hintergrundpapier_smart_home.pdf (21.10.2019).

[26] Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

gewährleisten, ist das Kopplungsverbot der DSGVO (vgl. Art. 7 DSGVO) zu berücksichtigen.

Überdies dürfen „smarte“ Spielzeuge nur nach ausdrücklichem Wunsch – z.B. durch einen Sprachbefehl oder einen Tastendruck – Daten aufzeichnen. Der Start der Aufzeichnung muss zudem deutlich gemacht werden. Dies kann beispielsweise durch visuelle oder auditive Zeichen geschehen. Anderenfalls könnte das Spielzeug – wie im Fall der Puppe Cayla – als eine verbotene, unbemerkte Sendeanlage nach §90 des Telekommunikationsgesetztes eingestuft und verboten werden.[27] Auch wenn die Hersteller der „smarten“ Spielzeuge dies beachten, können Drittanbieter über die Bereitstellung von Steuerungs-Apps Zugriff auf Kamera oder Mikrophon haben, die dem Nutzer nicht bewusst sind.[28] Die Hersteller sollten einen solchen Missbrauch soweit wie möglich unterbinden.

Kinder können das Konzept der Privatheit und des Datenschutzes zumeist noch nicht überblicken.[29] Deshalb ist bei smartem Spielzeug zudem durch eine entsprechende technische Gestaltung („Kindersicherung“) sicherzustellen, dass das Alter der Zugreifenden identifiziert wird, damit die Eltern die Kontrolle über die Datenschutzeinstellungen behalten und die rechtlichen Anforderungen der DSGVO an den Schutz Minderjähriger eingehalten werden.[30] Die Hersteller von Apps für „smarte“ Spielzeuge verweisen darauf, dass eine Kindersicherung des Smartphones ausreichend sei. In der Realität wird diese Sicherung von den Kindern jedoch häufig „geknackt“, weshalb ein entsprechender Authentifizierungsmechanismus zusätzlich notwendig ist.[31]

Auch sollte den Eltern klar sein, an wen die Daten weitergegeben werden, und sie sollten die Daten selbst verwalten und gegebenenfalls löschen können („Recht auf Vergessen werden“).[32] Dies gilt sowohl für alle Daten, die lokal auf dem Spielzeug gespeichert sind, als auch für Daten, die auf externen Servern der Hersteller gespeichert sind.[33]

---

[27] Bundesnetzagentur (2017): Bundesnetzagentur zieht Kinderpuppe „Cayla“ aus dem Verkehr. Abgerufen von: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html (21.10.2019).

[28] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

[29] Hung P.C., Fantinato, M., Rafferty, L. (2016). A Study of Privacy Requirements for Smart Toys. In PACIS Proceedings. 71.

[30] de Carvalho, L. G., Eler M., M. (2017). Security Requirements for Smart Toys. In ICEIS (2) (pp. 144-154).

[31] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

[32] de Carvalho, L. G., Eler M., M. (2017). Security Requirements for Smart Toys. In ICEIS (2) (pp. 144-154) und
Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

[33] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

Hieraus ergeben sich folgende Verbraucheranforderungen:

VA3: Die Verbindung von „smarten“ Spielzeugen zum Internet und anderen Geräten sollte einfach zu beenden sein.

VA4: Die Einstellung zur Datennutzung bei „smarten“ Spielzeugen sollten möglichst nutzerfreundlich ausgestaltet und datensparsam sein. Dazu müssen die DSGVO-Prinzipien des Privacy by design und Privacy by default berücksichtigt und verbraucherfreundlich ausgelegt werden.

VA5: Bei der Inbetriebnahme smarter Spielzeuge sowie bei Updates und sonstigen Veränderungen müssen die Eltern ausdrücklich der Datenübertragung und -nutzung zustimmen. Dabei muss eine informierte, differenzierte, freiwillige und widerrufbare Einwilligung ermöglicht werden.

VA6: Eine Aufnahme per Mikrophon oder Kamera darf nur nach bewusstem Befehl durch die Nutzerinnen und Nutzer erfolgen. Zudem muss immer deutlich erkennbar sein, wenn „smarte“ Spielzeuge Daten aufnehmen. Diese Anforderung gilt auch für Apps von Drittanbietern zur Steuerung von „smarten“ Spielzeugen.

VA7: Bei „smarten“ Spielzeugen ist sicherzustellen, dass die Datenschutzeinstellungen nur von den Eltern und nicht von den Kindern geändert werden können.

VA8: Die Eltern müssen Informationen über die Speicherung sowie eine mögliche Weitergabe der Nutzer- und Nutzungsdaten einfach und schnell ermitteln sowie die gespeicherten Daten selbst verwalten und löschen können („Recht auf vergessen werden“). Dies gilt sowohl für lokal auf dem „smarten“ Spielzeug gespeicherte Daten als auch auf externen Servern.

Das zweite Standbein dieses Leitwerts besteht in der **Datensicherheit**. Wie schon in VA 2 bei Leitwert 1 verdeutlicht wurde, kann das Hacken von „smarten“ Spielzeugen erhebliche negative Konsequenzen für die körperliche Sicherheit der Betroffenen haben.

Neben Gefahren für die gesundheitliche Unversehrtheit können Hacker auch Daten stehlen oder vernetzte Geräte wie „smarte“ Spielzeuge kapern, um diese als Teil eines Botnetzes zu missbrauchen.[34] Deshalb sollten vernetzte, „smarte“ Spielzeuge über sichere, verschlüsselte Verbindung zum Internet oder anderen

[34] Irish Times (2019). How to avoid silly mistakes with smart toys. Abgerufen von: https://www.irishtimes.com/business/technology/how-to-avoid-silly-mistakes-with-smart-toys-1.3893269 (21.10.2019) und
Internet Society (2017). This Holiday Season, Make Sure Your Smart Toys Isn’t a Toy Soldier. Abgerufen von: https://www.internetsociety.org/blog/2017/12/holiday-season-know-smart-toy-toy-soldier/ (21.10.2019).

vernetzten Geräten verfügen.[35] Von grundlegender Bedeutung sind hierbei die Verwendung sicherer Protokolle und Schnittstellen zur Verhinderung eines unbefugten Mitlesens bzw. einer unbefugten Nutzung (hierzu zählen u.a. sicher implementierte TSL-Verschlüsselungen sowie gesicherte WLAN- und Bluetooth-Verbindungen zwischen Produkt und Smartphone oder anderen Devices).

Im Fall eines Diebstahls oder Verlust des Spielzeugs können auch trotz einer sicheren, verschlüsselten Übertragungsverbindung Daten gestohlen und missbraucht werden. Deshalb sollte die Möglichkeit eines Zugriffschutzes gegeben und aktiviert sein.[36] Adäquate, sichere Authentifizierungsmechanismen für die Nutzung von „smarten“ Spielzeugen können sowohl den externen unerlaubten Zugriff über Verbindungen als auch die unerlaubte Nutzung im Falle eines Diebstahls verhindern. Deshalb sollten immer standardmäßig Passwörter vergeben sein, wenn die „smarten“ Spielzeuge auf den Markt kommen. Dafür sollten keine einfachen Default-Passwörter wie „0000“ oder „1234“ genutzt werden.[37] Dies gilt neben den „smarten“ Spielzeugen selbst auch für die zugehörigen Apps.

Die DSGVO fordert Unternehmen auf, die Datensicherheit ernst zu nehmen und geeignete technische und organisatorische Maßnahmen umzusetzen (Artikel 32).[38] Betriebssysteme sind in Abhängigkeit von den Funktionen des „smarten“ Spielzeugs unterschiedlich komplex gestaltet und sind die Grundlage für die Funktionalität eines „smarten“ Spielzeugs. Da mit steigender Komplexität auch die Fehleranfälligkeit eines Betriebssystems steigt, sollte es immer nur so komplex wie nötig gestaltet sein („Minimalprinzip“), da hier sonst ein Einfallstor für Kriminelle geschaffen wird (security by design).[39]

Erkenntnisse der Verbraucherforschung zeigen überdies, dass Verbraucherinnen und Verbraucher Voreinstellungen in der Regel beibehalten.[40] Deshalb sollten diese so voreingestellt sein, dass Datensicherheitsrisiken möglichst minimiert sind (security by default).

---

[35] Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

[36] Bundesamt für Sicherheit in der Informationstechnik (o.D.). Smartes Spielzeug – Lernhilfen oder Spion? Abgerufen von: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html (21.10.2019).

[37] Bundesamt für Sicherheit in der Informationstechnik (o.D.). Smartes Spielzeug – Lernhilfen oder Spion? Abgerufen von: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html (21.10.2019).

[38] Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

[39] Margraf, M. (2017). Datenschutz und -sicherheit in einer zunehmend vernetzten Welt. In Datenschutz und Datensicherheit, 41 (1), (pp. 21–23).

[40] Kettner, S. E., Thorun, C., Vetter, M. (2018). Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. Abgerufen von: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (21.10.2019).

Auch wenn die Spielzeuge beim Kauf diesen Kriterien entsprechen, können langfristig neue Gefahren für die Kinder entstehen. Deshalb sollten die Hersteller regelmäßig nach Sicherheitslücken suchen und es bedarf der langfristigen Bereitstellung automatischer, regelmäßiger Sicherheitsupdates durch die Anbieter, damit aufkommende Sicherheitslücken geschlossen werden können.[41] So sieht die EU-Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom Mai 2019 denn auch vor, dass Unternehmen Verbrauchern Sicherheitsaktualisierungen zur Verfügung stellen müssen.[42] Sofern ein Vertrag eine fortlaufende Bereitstellung digitaler Inhalte und Dienstleistungen über einen Zeitraum vorsieht, müssen diese während des gesamten Zeitraums vertragsgemäß sein und daher mit Sicherheitsupdates versorgt werden. Sofern der Vertrag lediglich eine einmalige Bereitstellung der Dienstleistung vorsieht, müssen Unternehmen Sicherheitsupdates so lange bereitstellen wie der Verbraucher es „vernünftigerweise“ erwarten kann (Artikel 8).[43]

Auch wenn die Daten auf dem „smarten“ Spielzeug sicher gespeichert sind und gegebenenfalls mit sicheren, verschlüsselten Übertragungsverbindung an die Server der Hersteller übermittelt wurden, so kann auch hier noch ein Sicherheitsrisiko bestehen. So gab es bereits mehrere Fälle, bei denen die Hersteller-Server gehackt und die gespeicherten Daten der Kinder gestohlen wurden: Ende 2015 wurden beispielsweise bei einem Angriff auf den Server des Kinderspielherstellers VTech 11,6 Millionen Nutzerkonten gehackt und persönliche Daten, Fotos sowie Sprachaufzeichnungen gestohlen.[44] Deshalb sollten die Server der Hersteller, auf denen die Daten der Kinder gespeichert und verarbeitet werden, adäquat gesichert sein.

Hieraus ergeben sich folgende Verbraucheranforderungen bezüglich der Datensicherheit:

VA9: „Smarte“ Spielzeuge sollten eine sichere, verschlüsselte Verbindung bzw. Datenübertragung zum Internet sowie Drittgeräten aufweisen.

VA10: „Smarte“ Spielzeuge sollten über adäquate, sichere Authentifizierungsmechanismen verfügen. Die Spielzeuge bzw. die zugehörigen Apps sollten immer per Default mit einem Passwort gesichert sein und dieses sollte hinreichend komplex sein.

---

[41] Bundesamt für Sicherheit in der Informationstechnik (o.D.). Smartes Spielzeug – Lernhilfen oder Spion? Abgerufen von: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html (21.10.2019) und
Verbraucherzentrale Bundesverband e.V. (2017). Hintergrundpapier des VZBV zum Thema Smart Home. Abgerufen von: https://www.vzbv.de/sites/default/files/downloads/2017/09/05/170905_hintergrundpapier_smart_home.pdf (21.10.2019).

[42] Richtlinie (EU) 2019/770 des Europäischen Parlaments und Rats vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0770&from=DE (22.10.2019).

[43] Hinweis: Ähnliche Anforderungen finden sich auch in der Richtlinie über vertragsrechtliche Aspekte des Warenhandels – Richtlinie für den Warenhandel, hier Artikel 7.

[44] Computerwoche.de (2017). My Friend Cayla, Hello Barbie &Co. – Kinderspiel(zeug) für Hacker. Abgerufen von: https://www.computerwoche.de/a/kinderspiel-zeug-fuer-hacker,3330077 (21.10.2019).

VA11: Security by design sollte bei der Entwicklung der Spielzeuge berücksichtigt werden. Unter anderem sollte das Betriebssystem von „smarten“ Spielzeugen immer nur so komplex wie nötig sein, da sonst unnötige Sicherheitslücken entstehen können („Minimalprinzip“).

VA12: Auch sollten die Sicherheitseinstellungen so voreingestellt sein, dass Risiken minimiert sind (security by default).

VA13: Für „smarte“ Spielzeuge müssen Sicherheitsupdates zur Verfügung gestellt werden, um die langfristige Sicherheit zu garantieren. Diese Pflicht besteht so lange Verbraucher dies „vernünftigerweise“ erwarten können. Hierfür müssen die Hersteller den Markt und ihre Produkte und Dienstleistungen regelmäßig auf Sicherheitslücken hin überprüfen.

VA14: Neben einer ausreichenden Sicherung der Daten auf dem „smarten“ Spielzeug müssen auch externe Server, auf denen Daten der Kinder gespeichert oder verarbeitet werden, adäquat gegen Cyberangriffe und Datendiebstahl geschützt sein.

3.2.3. Leitwert 3: Verhindern ökonomischer Nachteile für Verbraucher

Durch die Digitalisierung von Produkten sind für Verbraucherinnen und Verbraucher eine Vielzahl an neuen Möglichkeiten entstanden, insbesondere bei vernetzten Geräten. Gleichzeitig ist die Nutzung dieser Produkte und der zugehörigen Dienstleistung deutlich günstiger geworden.

Allerdings gibt es auch mögliche ökonomische Nachteile bei der Nutzung vernetzter Geräte wie „smarten“ Spielzeugen. Wenn ein „smartes“ Spielzeug durch die Interaktion lernt und sich an das Kind anpasst, so bekommt es für das Kind einen höheren Nutzen. Wenn das Kind nun ein ähnliches Gerät eines anderen Anbieters oder ein Nachfolgermodell nutzen möchte, so sollte es die Daten und die „Weiterentwicklung“ der Software auch in diesem neuen „smarten“ Spielzeug nutzen können. Eine solche Bereitstellung der Daten „in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format“ fordert auch die DSGVO.[45] Deshalb muss eine Datenportabilität zwischen vergleichbaren „smarten“ Spielzeugen gewährleistet sein, damit keine Lock-In-Effekte entstehen. Der Anspruch an Interoperabilität gilt auch für die Verbindung mit anderen vernetzten Geräten des Internet of Things. Hierfür bedarf es einheitlicher Standards für die Kommunikation und Datenübertragbarkeit zwischen den Geräten.[46]

[45] Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679 (21.10.2019).

[46] Verbraucherzentrale Bundesverband e.V. (2017). Hintergrundpapier des VZBV zum Thema Smart Home. Abgerufen von: https://www.vzbv.de/sites/default/files/downloads/2017/09/05/170905_hintergrundpapier_smart_home.pdf (21.10.2019).

Auch können Kosten entstehen, wenn im Rahmen der Nutzung eines Spielzeugs weitere Dienste angeboten werden, die durch In-App-Käufe umgesetzt werden. Diese Kosten sind für die Verbraucher nicht immer transparent. Insbesondere bei smartem Spielzeug, das vorrangig von Kindern genutzt wird, ist die Gefahr von ungeahnten Zusatzkosten durch scheinbar kostenlose Zusatzleistungen besonders groß.[47] Deshalb sollte – wie beim Zugriff auf die Datenschutzeinstellungen – vor jedem Kauf von Zusatzleistungen eine Authentifizierung durch einen Erziehungsberechtigten stattfinden.[48]

Zudem sollten die Daten der Kinder beim Spielen mit „smartem“ Spielzeug nicht zur Profilbildung für Marketingzwecke genutzt werden.[49] Einige Geschäftsmodelle beruhen darauf, dass eine Leistung zwar kostenlos erbracht wird, dass die Verbraucherinnen und Verbraucher aber letztlich mit ihren Daten zahlen. Dies sollte bei Kindern unter 16 Jahren als Nutzerinnen und Nutzer der „smarten“ Spielzeuge nicht ohne Einwilligung der Erziehungsberechtigten möglich sein.[50]

Bei diesem Leitwert gibt es allerdings auch einen Zielkonflikt zwischen einer hohen Interoperabilität und dem Schutz von Kindern.[51] So soll die Vernetzung und Interoperabilität von „smarten“ Spielzeugen aus ökonomischer Sicht für die Verbraucher leicht gemacht werden, aus Sicht des Jugendschutzes sollte sie hingegen nicht zu einfach sein (z.B. strenge Authentisierungsmechanismen zum Schutz der Kinder).

Aus diesen Punkten ergeben sich folgende Verbraucheranforderungen im Rahmen dieses Leitwerts:

> **VA15:** Es muss sichergestellt werden, dass keine Lock-in-Effekte entstehen. Dazu muss die Datenportabilität zwischen vergleichbaren „smarten“ Spielzeugen gewährleistet sein. Auch eine Interoperabilität mit anderen vernetzten Geräten sollte möglich sein, wofür einheitliche Standards notwendig sind.

---

[47] Securitymadein.lu (o.D.). Smart Toys, Multiple Facetten, Multiple Risiken. Abgerufen von: https://www.bee-secure.lu/sites/default/files/publications/Article_Jouets_connectes-DE_UA.pdf (21.10.2019).
[48] de Carvalho, L. G., Eler M., M. (2017). Security Requirements for Smart Toys. In ICEIS (2) (pp. 144-154).
[49] Verbraucherschutz-Minister Konferenz (24.05.2019). Top 17: Smart Toys – Daten- und verbraucherschützende Vorkehrungen für besonders schutzwürdige Verbraucher(innen) treffen Abgerufen von: https://www.verbraucherschutzministerkonferenz.de/documents/ergebnisprotokoll-der-15-vsmk-am-24052019-in-mainz_rlp-extern_1559902425.pdf (21.10.2019) und
Verbraucherzentrale.de (2018). Vorsicht bei Smart Toys: Die Risiken von vernetztem Spielzeug. Abgerufen von: https://www.verbraucherzentrale.de/aktuelle-meldungen/umwelt-haushalt/vorsicht-bei-smart-toys-die-risiken-von-vernetztem-spielzeug-29297 (21.10.2019) und
Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.
[50] Klicksafe.de (o.D.). Vernetztes Spielzeug – Dateschutzrisiko im Kinderzimmer. Abgerufen von: https://www.klicksafe.de/eltern/kinder-von-3-bis-10-jahren/vernetztes-spielzeug/ (21.10.2019).
[51] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

VA16: Die Kinder als Nutzer sollten vor (versteckten) Kosten durch In-App-Käufe geschützt werden (z.B. durch erneute Authentifizierung durch die Eltern vor In-App-Käufen).

VA17: Die Kinder sollten vor der Nutzung ihrer Daten zu Marketingzwecken geschützt werden. Das Geschäftsmodell „Daten gegen Leistung“ sollte bei „smarten“ Spielzeugen nur bei Einwilligung der Erziehungsberechtigten möglich sein.

3.2.4. Leitwert 4: Gebrauchstauglichkeit und Qualität von Produkten und Dienstleistungen

Wie in Kapitel 3.1 gezeigt lässt die Digitalisierung die Grenzen zwischen Produkten und Dienstleistungen immer mehr verschwimmen und es entstehen häufig „hybride“ Produkte, die über einen Cloud-Dienst eine Dienstleistung zur Verfügung stellen. Somit muss ein breiteres Verständnis von Gebrauchstauglichkeit und Qualität entwickelt werden, das z.B. auch die in VA15 genannten Punkte der Datenportabilität und Interoperabilität umfasst.

Deshalb sollten sich Gewährleistungsansprüche und Garantien für „smartes“ Spielzeug nicht nur auf das physische Produkt, sondern auch auf die dazugehörige Dienstleistung – z.B. die „intelligente“ Interaktion des Spielzeugs mit dem Kind – erstrecken.[52]

Überdies ist dafür Sorge zu tragen, dass Gewährleistungsansprüche auch dann greifen, wenn Verbraucher digitale Güter nicht mit Geld, sondern im Gegenzug zu ihren Daten erhalten. So sieht die EU-Richtlinie für digitale Inhalte genau diesbezüglich eine Klarstellung vor.[53]

Updates von Betriebssystemen können dazu führen, dass Produkte an Gebrauchswert verlieren, da die Hardware überfordert ist. Funktionale Updates, die nicht sicherheitsrelevant sind, sollten von den Herstellern demnach immer optional angeboten werden.[54] Auch sollten Updates einfach zu installieren sein und die Geräte für die Installation von Updates ausgelegt und „Update-fähig“ sein.[55]

Auch sollten elektronische Verschleißteile wie Displays oder Akkus durch die Eltern einfach austauschbar sein, da gerade bei der Nutzung von smartem Spielzeug

---

[52] Verbraucherzentrale Bundesverband e.V. (2017). Hintergrundpapier des VZBV zum Thema Smart Home. Abgerufen von: https://www.vzbv.de/sites/default/files/downloads/2017/09/05/170905_hintergrundpapier_smart_home.pdf (21.10.2019) und
Securitymadein.lu (o.D.). Smart Toys, Multiple Facetten, Multiple Risiken. Abgerufen von: https://www.bee-secure.lu/sites/default/files/publications/Article_Jouets_connectes-DE_UA.pdf (21.10.2019).

[53] Richtlinie (EU) 2019/770 des Europäischen Parlaments und Rats vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019L0770&from=DE (22.10.2019).

[54] Information des DIN-Verbraucherrates (2019). Digitale Sicherheit – Updates. Abgerufen von: https://www.din.de/resource/blob/327068/bdbd65d87754971cff7cb86dfe310c49/information-des-din-vr-digitale-sicherheit-updates-data.pdf (21.10.2019).

[55] Anmerkungen einer Expertin bzw. eines Experten im Interview.

durch Kinder häufig Teile kaputt gehen und beschädigt werden.[56] Hier besteht jedoch ein Spannungsfeld, da Batterien nicht zu leicht – also ohne Zuhilfenahme eines Werkzeuges (siehe DIN EN 62115) – auszubauen sein sollten, damit Kinder sich nicht daran verletzen, etwa indem sie Kleinteile wie Batterien verschlucken. Zudem sollten Displays eine gewisse Haltbarkeit aufweisen und entsprechend stabil konstruiert sein, da Kinder zumeist nicht sehr sorgsam mit Spielzeugen umgehen.[57]

Hersteller sollten auf eine einfache Bedienbarkeit und Barrierefreiheit bei Steuerungsmodulen wir Touchscreens oder Spracheingabesysteme achten, da die Gebrauchstauglichkeit der „smarten“ Spielzeuge in hohem Maße von einer einfachen Steuerung abhängt. Dies gilt insbesondere für Kinder mit Behinderungen oder anderen Einschränkungen.[58]

VA18: Gewährleistungsansprüche für „smarte“ Spielzeuge sollten auch für alle zugehörigen Dienstleistungen gelten, die für die Nutzung des „smarten“ Spielzeugs benötigt werden.

VA19: Gewährleistungsansprüche müssen auch dann gelten, wenn Verbraucher digitale Güter nicht mit Geld bezahlen, sondern im Gegenzug für ihre Daten erhalten.

VA20: Produkt-Updates sollten optional angeboten werden, falls sie nicht sicherheitsrelevant sind. Auch müssen die Geräte „updatefähig“ sein und die Installation der Updates für die Nutzer muss einfach gestaltet sowie ohne technisches Wissen durchführbar sein.

VA21: Elektronische Verschleißteile wie Batterien, Akkus und Displays sollten möglichst einfach ausgetauscht werden können, aber gleichzeitig für die Kinder nicht erreichbar (Batterien und Akkus) bzw. „Kinderfest“ (Displays) sein.

VA22: Hersteller sollten darauf achten, dass die „smarten“ Spielzeuge barrierefrei zu bedienen sind. Dies gilt insbesondere auch für die Nutzung durch Kinder mit Behinderungen oder anderen Einschränkungen.

3.2.5. Leitwert 5: Prinzipien der Nachhaltigkeit

Nachhaltiges Verhalten – sowohl in ökologischer als auch sozialer Sicht – ist heute für viele Verbraucherinnen und Verbraucher ein zentrales Anliegen bei der

[56] Consumers International (2019). Consumer IoT: Trust be Design 2019: Guidelines and Checklists. Abgerufen von: https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf (21.10.2019) und
European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) & The European Consumer Organisation (BEUC) (2018). Cybersecurity for Connected Products. Abgerufen von: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf (21.10.2019).

[57] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

[58] ConPolicy (2018): Entwicklung eines strategischen Konzepts zum Umgang mit der Digitalisierung in der Normung im Auftrag des DIN-Verbraucherrats.

Wahl eines Produktes. Bei „smarten“ Spielzeugen kommt diesem Punkt durch die Kombination von Spielzeugtechnik und Dienstleistung eine spezielle Bedeutung zu. Dies wird schon durch **VA20** (Produktupdates) und **VA21** (Austauschbarkeit von Teilen) deutlich, die sich neben der Gebrauchstauglichkeit auch auf den Leitwert der Nachhaltigkeit beziehen.

Die Ökodesign-Richtlinie von 2009[59] sowie die WEEE-Richtlinie von 2012[60] der EU besagen zudem, dass Verbraucherinnen und Verbraucher vor dem Kauf wissen müssen, wie energieeffizient ein Spielzeug ist. In der Nutzungsphase müssen sie wissen, wie sie das Spielzeug energiesparsam nutzen können und nach der Nutzungsphase müssen sie wissen, wie sie es fachgerecht entsorgen. Deshalb müssen die Hersteller in der Produktinformation die Energieeffizienz angeben und Leitlinien für die energieeffiziente Nutzung und Entsorgung mitgeben.[61]

Auch verlangt die Ökodesign-Richtlinie die „smarten“ Spielzeuge so zu gestalten, dass sie automatisch in den Zeiträumen Energie sparen, in denen sie wenig genutzt werden – z.B. nachts, wenn das Kind schläft.[62] Solche nachhaltigen und energiesparenden Einstellungen sollten schon per Default voreingestellt sein, da viele Verbraucherinnen und Verbraucher Voreinstellungen nachträglich nicht mehr verändern (siehe VA12).[63]

Somit resultieren bezüglich der Nachhaltigkeit folgende Verbraucheranforderungen:

VA23: Die Hersteller müssen in der Produktinformation die Energieeffizienz kennzeichnen und mit den Produkten Leitlinien für eine effiziente Nutzung und Entsorgung von „smarten“ Spielzeugen bereitstellen.

VA24: „Smarte“ Spielzeuge müssen so konstruiert sein, dass sie in bestimmten, wenig genutzten Zeiträumen automatisch Energie sparen. Dies sollte

---

[59] Richtlinie 2009/125/EG des Europäischen Parlaments und des Rates zur Schaffung eines Rahmens für die Festlegung von Anforderungen an die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte. Abgerufen unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:285:0010:0035:DE:PDF (21.10.2019).

[60] Richtlinie 2012/19/EU des Europäischen Parlaments und Rates über Elektro- und Elektronik-Altgeräte. Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012L0019&from=DE (21.10.2019).

[61] Consumers International (2019). Consumer IoT: Trust be Design 2019: Guidelines and Checklists. Abgerufen von: https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf (21.10.2019) und
European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) & The European Consumer Organisation (BEUC) (2018). Cybersecurity for Connected Products. Abgerufen von: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf (21.10.2019).

[62] European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) & The European Consumer Organisation (BEUC) (2018). Cybersecurity for Connected Products. Abgerufen von: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf (21.10.2019).

[63] Thorun, C., Diels, J., Vetter, M., Reisch, L., Bernauer, M., Micklitz, H. W. & Sunstein, C. R. (2016). Nudge-Ansätze beim nachhaltigen Konsum: Ermittlung und Entwicklung von Maßnahmen zum „Anstoßen“ nachhaltiger Konsummuster. Abschlussbericht für den Umweltforschungsplan des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit, Forschungskennzahl, 3714(93), 303.

schon in den Werkseinstellungen berücksichtigt werden (Energiesparsamkeit by Default).

3.2.6. Leitwert 6: Herstellung von Transparenz und Vergleichbarkeit auf Märkten

Verbraucherinnen und Verbraucher treffen ihre Entscheidungen insbesondere auf Basis der ihnen zur Verfügung stehenden Informationen. Bei der Entscheidung über den Kauf eines „smarten“ Spielzeugs kommt der transparenten Darstellung von vorvertraglichen Informationen zum Datenschutz – insbesondere der Verarbeitung und Weitergabe von Daten – eine besondere Bedeutung zu, da es sich um vernetzte Geräte handelt.

Deshalb sollten die Nutzungsbedingungen diesbezüglich klar, übersichtlich und verständlich gestaltet und einfach zu finden sein.[64] Um eine verständliche Aufarbeitung und Darstellung der Datenschutzbestimmungen zu ermöglichen, sollten sie zudem optimalerweise maschinenauslesbar sein, so dass Verbraucherinnen und Verbraucher Dienste zum Auslesen und Vergleich von Datenschutzbestimmungen nutzen können.[65]

Viele „smarte“ Spielzeuge kommunizieren mit den Kindern, lernen aus deren Verhalten und passen die Reaktionen dementsprechend an. Dafür werden häufig algorithmische Systeme eingesetzt. Die Hersteller sollten dies verpflichtend angeben und über die Funktionsweise in einer klar verständlichen Art und Weise aufklären.[66] In Bezug auf den Einsatz von algorithmischen Systemen forderte EU-Wettbewerbskommissarin Margrethe Vestager das Prinzip des „trust by design“ zu fördern.[67] Auch spricht sich die Datenethikkommission in ihren Handlungsempfehlungen an die Bundesregierung u.a. dafür aus, dass Hersteller beim Einsatz von

---

[64] Consumers International (2019). Consumer IoT: Trust be Design 2019: Guidelines and Checklists. Abgerufen von: https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf (21.10.2019) und
European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) & Bureau Européen des Unions de Consommateurs (BEUC) (2018). Cybersecurity for Connected Products. Abgerufen von: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf (21.10.2019) und
Moll R., Scheibel L., Rusch-Rodosthenous M. (2018). Vernetztes Kinderspielzeug – Datenrisiko im Kinderland? In: Marktwächter Digitale Welt (p. 4). Verbraucherzentrale NRW e.V., Düsseldorf.

[65] Kettner, S. E., Thorun, C., Vetter, M. (2018). Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. Abgerufen von: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (21.10.2019) und
SVRV (2017). Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Abgerufen von: http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souver%C3%A4nit%C3%A4t_.pdf (21.10.2019)

[66] SVRV (2018). Verbrauchergerechtes Scoring. Gutachten des Sachverständigenrats für Verbraucherfragen. Abgerufen von: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf (21.10.2019).

[67] Heise online (2019). EU-Kommission: Digitalchefin Vestager plädiert bei KI für „Vertrauen by Design“. Abgerufen von: https://www.heise.de/newsticker/meldung/EU-Kommission-Digitalchefin-Vestager-plaediert-bei-KI-fuer-Vertrauen-by-Design-4549502.html (21.10.2019).

algorithmischen Systemen eine Risikofolgenabschätzung durchführen, deren Einsatz kennzeichnen und gewährleisten, dass Algorithmen basierte Entscheidungen erklärbar sind.[68]

Ebenfalls vorvertraglich sollten Informationen zu Lebenszeit, Updatefähigkeit und Energieeffizienz bereitgestellt werden.[69] Es sollte zudem klar dargestellt werden, ob die Geräte auch nicht-vernetzt genutzt werden können und ob Apps bzw. Konten zur Nutzung benötigt werden.[70] Auch die Notwendigkeit der Inanspruchnahme von Zusatzdienstleistungen für die Nutzung des „smarten“ Spielzeugs sollte klar kommuniziert werden.[71]

Die Digitalisierung und Vernetzung hat für diesen Leitwert demnach die folgenden Konsequenzen:

VA25: Die Nutzungsbestimmung und die Regelungen zur Verarbeitung und Weitergabe von Daten sollten einfach zugänglich und transparent gestaltet sein. Zudem würden maschinenauslesbare Datenschutzerklärungen die Vergleichbarkeit für die Verbraucherinnen und Verbraucher erhöhen.

VA26: Die Anbieter von „smarten“ Spielzeugen sollten verpflichtend kennzeichnen müssen, wenn sie algorithmische Systeme nutzen und über deren Funktionsweise aufklären.

VA27: Relevante vorvertragliche Informationen sollten vergleichbar und transparent dargestellt werden. Dies betrifft etwa die erwartete Dauer der Updatebereitstellung, die Reparaturfähigkeit, die Energieeffizienz sowie die Notwendigkeit von Apps oder zusätzlichen Dienstleistungen für die Nutzung.

3.2.7. Leitwert 7: Schutz vor Täuschung

Verbraucherinnen und Verbraucher haben durch die Digitalisierung immer mehr Zugang zu Informationen, was ihnen eine bessere und fundiertere Entscheidung ermöglichen kann (siehe insb. Verbraucheranforderungen der Leitwerte 3 und 6), wenn diese Informationen entsprechend verfügbar und verständlich dargestellt sind. Jedoch entstehen – wie beschrieben – mit dem Aufkommen „hybrider“ Produkte auch unübersichtlichere Produkte und Geschäftsmodelle, die Täuschung und Betrug von Verbraucherinnen und Verbrauchern vereinfachen bzw. teilweise

---

[68] Datenethikkommission (2019). Gutachten der Datenethikkommission. Abgerufen von: https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf (23.10.2019), Kapitel F.

[69] Consumers International (2019). Consumer IoT: Trust be Design 2019: Guidelines and Checklists. Abgerufen von: https://www.consumersinternational.org/media/239715/trust-by-design-guidelines.pdf (21.10.2019) und
European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) & Bureau Européen des Unions de Consommateurs (BEUC) (2018). Cybersecurity for Connected Products. Abgerufen von: http://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2018-G-001final.pdf (21.10.2019).

[70] Anmerkungen einer Expertin bzw. eines Experten im Interview

[71] Securitymadein.lu (o.D.). Smart Toys, Multiple Facetten, Multiple Risiken. Abgerufen von: https://www.bee-secure.lu/sites/default/files/publications/Article_Jouets_connectes-DE_UA.pdf (21.10.2019).

erst ermöglichen. Diese Gefahr besteht bei „smarten“ Spielzeugen insbesondere bei Zusatzleistungen oder In-App-Käufen, über deren Kosten nicht adäquat informiert wird bzw. die den Anschein erwecken, kostenlos zu sein (siehe **VA16**). Auch können Daten weitergegeben werden, obwohl die Verbraucherinnen und Verbraucher nicht eingewilligt haben (siehe **VA5**). Wenn die bereits oben beschriebenen Verbraucheranforderungen eingehalten werden, besteht automatisch ein gewisser Schutz vor Täuschung. Deshalb wird bei diesem Leitwert von einer Formulierung weiterer Verbraucheranforderungen abgesehen.

3.2.8. Leitwert 8: Interessen besonders schutzbedürftiger gesellschaftlicher Gruppen

Im Gegensatz zu anderen vernetzen Geräten stellt sich bei „smarten“ Spielzeugen eine besondere Situation dar: Hier sind Kinder zumeist die Nutzerinnen und Nutzer der Spielzeuge und die Absender von Daten. Die Entscheidung über den Kauf und die Art der Nutzung eines „smarten“ Spielzeugs treffen jedoch zumeist die Eltern bzw. die Erziehungsberechtigten. Dies wird auch in den zuvor formulierten Verbraucheranforderungen deutlich: Die in **VA7** gestellte Forderung nach einer „Kindersicherung“ bei der Datenschutzeinstellung ergibt sich genauso aus der besonderen Schutzwürdigkeit von Kindern, wie der Schutz vor versteckten Kosten durch In-App-Käufe durch Kinder (**VA16**) oder die Forderung nach einem Verbot der Verwertung der Nutzungsdaten für Marketingzwecke (**VA17**). Die barrierefreie Bedienbarkeit von „smarten“ Spielzeugen für Kinder mit Behinderungen oder Einschränkungen ist schon in Form von **VA22** formuliert worden.

Ein weiterer Aspekt, der für Kinder als besonders schutzwürdige gesellschaftliche Gruppe relevant ist, und der in den oben genannten Verbraucheranforderungen noch nicht adressiert wurde, ist die Kommunikation zwischen Nutzern von „smarten“ Spielzeugen, etwa über Chatfunktionen. Falls „smarte“ Spielzeuge über solche Funktionen verfügen, muss durch eine Moderation des Chats sichergestellt werden, dass z.B. pornographische oder rassistische Inhalte nicht auftauchen bzw. schnellstmöglich gelöscht werden.[72]

Daraus ergibt sich für diesen Leitwert folgende zusätzliche Verbraucheranforderung:

> **VA28:** Die Anbieter von Dienstleistungen für „smarte“ Spielzeuge, die Chatfunktionen umfassen, müssen sicherstellen, dass keine jugendgefährdenden Inhalte über diese Chatfunktion geteilt und verbreitet werden. Eine Lösung hierfür ist eine professionelle Moderation des Chats.

[72] Beitrag aus dem Fachgespräch vom 23.09.2019 zum Thema „Digitalisierungsaspekte und Verbraucheranforderungen in Bezug auf „smartes Spielzeug“ – Umsetzung in der Normung.“ Deutsches Institut für Normung, Berlin.

3.2.9. Zwischenfazit zu den Verbraucheranforderungen

Eine Betrachtung der identifizierten Verbraucheranforderungen zeigt, dass grundsätzlich zwischen zwei Typen von Verbraucheranforderungen unterschieden werden kann: Einerseits beziehen sich viele der beschriebenen Verbraucheranforderungen auf vernetzte Geräte allgemein und gelten somit nicht nur für „smarte“ Spielzeuge, sondern etwa auch für „smarte“ Drucker, Sprachassistenten oder Smartphones. Einige andere Verbraucheranforderungen betrachten hingegen spezifisch „smarte“ Spielzeuge – zumeist, weil Kinder als Nutzer eine spezielle Zielgruppe darstellen – und sind für andere vernetzte Geräte nicht relevant.

Die Unterscheidung zwischen diesen beiden Typen an Verbraucheranforderungen ist aus zwei Gründen von Bedeutung: Zunächst hängt davon ab, in welcher Art von Normen und Spezifikationen entsprechende Inhalte zu erwarten sind. Verbraucheranforderungen an vernetzte Geräte allgemein werden eher in Normen und Spezifikationen für Konsumgeräte des Internet of Things zu finden sein, während spezifisch an „smartes“ Spielzeug gerichtete Verbraucheranforderungen in Spielzeugnormen zu vermuten sind. Zudem hängt zweitens auch die Entwicklung der Handlungsempfehlungen für die Normungsarbeit in Kapitel 5 stark davon ab, ob Verbraucheranforderungen vernetzte Geräte allgemein oder spezifisch Spielzeug betreffen. Dies liegt darin begründet, dass die Normen in verschiedenen Gremien entwickelt werden und die Ansprechpartner sich stark unterscheiden – je nachdem, ob es sich um Normen für IoT-Geräte allgemein oder für Spielzeug im Speziellen handelt. Deshalb werden die 28 Verbraucheranforderungen in der folgenden Tabelle nach dieser Unterscheidung eingeteilt und dargestellt.

Allgemeine Verbraucheranforderungen an vernetzte Geräte	Spezifische Verbraucheranforderungen an „smarte“ Spielzeuge
VA2: Eine unbefugte Kontaktaufnahme durch Dritte und Manipulation der Kinder über einen **unerlaubten Fernzugriff**, die zu einer physischen oder psychischen Schädigung führen kann, muss ausgeschlossen sein.	**VA1:** Von „smarten“ Spielzeugen dürfen **keine Gefahr** durch elektrische Schläge, elektromagnetische Strahlung oder selbständigen Bewegungen des Spielzeugs ausgehen. Zudem dürfen durch Bildschirme keine Sehstörungen bei Kindern entstehen und es bedarf Höchstwerten bezüglich der Geräuschbelastung.
VA3: Die **Verbindung** von „smarten“ Spielzeugen zum Internet und anderen Geräten sollte **einfach zu beenden** sein.	**VA7:** Bei „smarten“ Spielzeugen ist sicherzustellen, dass die **Datenschutzeinstellungen** nur von den Eltern und **nicht von den Kindern geändert** werden können.
VA4: Die **Einstellung zur Datennutzung** bei „smarten“ Spielzeugen sollten möglichst **nutzerfreundlich** ausgestaltet und datensparsam sein. Dazu müssen die DSGVO-Prinzipien des Privacy by design und Privacy by default berücksichtigt und verbraucherfreundlich ausgelegt werden.	**VA16:** Die Kinder als Nutzer sollten **vor (versteckten) Kosten durch In-App-Käufe geschützt** werden (z.B. durch erneute Authentifizierung durch die Eltern vor In-App-Käufen).
VA5: Bei der Inbetriebnahme smarter Spielzeuge sowie bei Updates und sonstigen Veränderungen müssen die Eltern ausdrücklich der Datenübertragung und -nutzung zustimmen. Dabei muss **eine informierte, differenzierte, freiwillige und widerrufbare Einwilligung** ermöglicht werden.	**VA17:** Die Kinder sollten vor der Nutzung ihrer **Daten zu Marketingzwecken geschützt** werden. Das Geschäftsmodell „Daten gegen Leistung“ sollte bei „smarten“ Spielzeugen nur bei Einwilligung der Erziehungsberechtigten möglich sein.
VA6: Eine Aufnahme per Mikrophon oder Kamera darf nur nach bewusstem Befehl durch die Nutzerinnen und Nutzer erfolgen. Zudem muss immer deutlich erkennbar sein, wenn „smarte“ Spielzeuge Daten aufnehmen. Diese Anforderung gilt auch für Apps von Drittanbietern zur Steuerung von „smarten“ Spielzeugen.	**VA21: Elektronische Verschleißteile** wie Batterien, Akkus und Displays sollten möglichst **einfach ausgetauscht** werden können, aber gleichzeitig **für die Kinder nicht erreichbar** sein (Batterien und Akkus) bzw. „Kinderfest“ (Displays) sein.
VA8: Die Eltern müssen Informationen über die Speicherung sowie eine mögliche Weitergabe der Nutzer- und Nutzungsdaten einfach und schnell ermitteln sowie die **gespeicherten Daten selbst verwalten und löschen können** („Recht auf vergessen werden“). Dies gilt sowohl für lokal auf dem „smarten“ Spielzeug gespeicherte Daten als auch auf externen Servern.	**VA22:** Hersteller sollten darauf achten, dass die **„smarten“ Spielzeuge barrierefrei** zu bedienen sind. Dies gilt insbesondere auch für die Nutzung durch Kinder mit Behinderungen oder anderen Einschränkungen.
VA9: „Smarte“ Spielzeuge sollten eine **sichere, verschlüsselte Verbindung bzw. Datenübertragung** zum Internet sowie Drittgeräten aufweisen.	**VA28:** Die Anbieter von Dienstleistungen für „smarte“ Spielzeuge, die Chatfunktionen umfassen, müssen sicherstellen, dass **keine jugendgefährdenden Inhalte über** diese **Chatfunktion** geteilt und verbreitet werden. Eine Lösung hierfür ist eine professionelle Moderation des Chats.
VA10: „Smarte“ Spielzeuge sollten über **adäquate, sichere Authentifizierungsmechanismen** verfügen. Die Spielzeuge bzw. die zugehörigen Apps sollten immer per Default mit einem Passwort gesichert sein und dieses sollte hinreichend komplex sein.	
VA11: Security by design sollte bei der Entwicklung der Spielzeuge berücksichtigt werden. Unter anderem sollte das Betriebssystem von „smarten“ Spielzeugen immer nur so komplex wie nötig sein, da sonst unnötige Sicherheitslücken entstehen können („Minimalprinzip“).	
VA12: Auch sollten die Sicherheitseinstellungen so voreingestellt sein, dass Risiken minimiert sind (**security by default**).	
VA13: Für „smarte“ Spielzeuge müssen **Sicherheitsupdates zur Verfügung** gestellt werden, um die langfristige Sicherheit zu garantieren. Diese Pflicht besteht so lange Verbraucher dies „vernünftigerweise“ erwarten können. Hierfür müssen die Hersteller den Markt und ihre Produkte und Dienstleistungen regelmäßig auf Sicherheitslücken hin überprüfen.	
VA14: Neben einer ausreichenden Sicherung der Daten auf dem „smarten“ Spielzeug müssen auch **externe Server**, auf denen Daten der Kinder gespeichert oder verarbeitet werden, adäquat gegen Cyberangriffe und Datendiebstahl **geschützt** sein.	
VA15: Es muss sichergestellt werden, dass **keine Lock-in-Effekte** entstehen. Dazu muss die Datenportabilität zwischen vergleichbaren „smarten“ Spielzeugen gewährleistet sein. Auch eine Interoperabilität mit anderen vernetzten Geräten sollte möglich sein, wofür einheitliche Standards notwendig sind.	
VA18: Gewährleistungsansprüche für „smarte“ Spielzeuge sollten auch **für alle zugehörigen Dienstleistungen** gelten, die für die Nutzung des „smarten“ Spielzeugs benötigt werden.	
VA19: Gewährleistungsansprüche müssen auch dann gelten, wenn Verbraucher digitale Güter nicht mit Geld bezahlen, sondern **im Gegenzug für ihre Daten** erhalten.	
VA20: Produkt-Updates sollten optional angeboten werden, falls sie nicht sicherheitsrelevant sind. Auch müssen die Geräte „updatefähig“ sein und die Installation der Updates für die Nutzer muss einfach gestaltet sowie ohne technisches Wissen durchführbar sein.	
VA23: Die Hersteller müssen in der **Produktinformation** die Energieeffizienz kennzeichnen und mit den Produkten Leitlinien für eine effiziente Nutzung und Entsorgung von „smarten“ Spielzeugen bereitstellen.	
VA24: „Smarte“ Spielzeuge müssen so konstruiert sein, dass sie in bestimmten, wenig genutzten Zeiträumen **automatisch Energie sparen**. Dies sollte schon in den Werkseinstellungen berücksichtigt werden (Energiesparsamkeit by Default).	
VA25: Die **Nutzungsbestimmung** und die Regelungen zur **Verarbeitung und Weitergabe von Daten** sollten **einfach zugänglich und transparent** gestaltet sein. Zudem würden maschinenauslesbare Datenschutzerklärungen die Vergleichbarkeit für die Verbraucherinnen und Verbraucher erhöhen.	
VA26: Die Anbieter von „smarten“ Spielzeugen sollten **verpflichtend kennzeichnen** müssen, wenn sie **algorithmische Systeme** nutzen und über deren Funktionsweise aufklären.	
VA27: Relevante **vorvertragliche Informationen** sollten vergleichbar und **transparen**t dargestellt werden. Dies betrifft etwa die erwartete Dauer der Updatebereitstellung, die Reparaturfähigkeit, die Energieeffizienz sowie die Notwendigkeit von Apps oder zusätzlichen Dienstleistungen für die Nutzung.	

Tabelle 1: Einteilung: Allgemeine Verbraucheranforderungen an vernetzte Geräte und spezifische Verbraucheranforderungen an „smarte“ Spielzeuge

4. Identifikation von Normen und Abgleich mit den Verbraucheranforderungen

4.1. Identifikation relevanter Normen für „smarte” Spielzeuge

Normen und Standards beschreiben bestimmte Richtlinien für die Konstruktion von Produkten oder für das Anbieten von Dienstleistungen. Da – wie zuvor dargelegt – durch die Digitalisierung die Grenze zwischen Produkten und Dienstleistungen verschwimmt, entstehen „hybride“ Produkte mit Dienstleistungskomponenten. Zu diesen zählen auch „smarte“ Spielzeuge. Dadurch entstehen neben den neuen Verbraucheranforderungen auch neue Herausforderungen für die Normungsarbeit, da nicht mehr immer klar zwischen Produkt- und Dienstleistungsnormung getrennt werden kann. Zudem wurde in Kapitel 3 deutlich, dass sich manche Verbraucherforderungen spezifisch auf Spielzeuge – bzw. die Kinder als Nutzer von Spielzeugen – beziehen, während andere Verbraucheranforderungen für alle vernetzten Produkte des Internet of Things gelten. Deshalb können die zuvor identifizierten Verbraucheranforderungen sowohl in spezifischen Spielzeugnormen adressiert sein als auch in Normen, die für vernetzte Geräte im Allgemeinen gelten.

Durch die Recherche in der Online-Normendatenbank von Beuth, der Recherche im Internet, Gesprächen mit der Geschäftsstelle des DIN-VR sowie den Interviews mit den Expertinnen und Experten konnten folgende Normen oder Spezifikationen identifiziert werden, die für die hergeleiteten Verbraucheranforderungen relevant sein könnten:

- **DIN EN 71-1**: Sicherheit von Spielzeug - Mechanische und physikalische Eigenschaften:

  Diese Norm ist die „klassische“ Spielzeugsicherheitsnorm. Sie beschreibt wie analoge Spielzeuge beschaffen sein sollten, so dass sie für die Kinder als Nutzer keine Gefahr darstellen.

- **DIN EN 62115**: Elektrische Spielzeuge - Sicherheit

  Diese Norm bezieht sich spezifisch auf Spielzeuge, die elektrisch betrieben werden. Sie behandelt die Sicherheit von elektrischen Spielzeugen, die mindestens eine von Elektrizität abhängende Funktion besitzen.

- **ETSI TS 103 645**: Cyber Security for Consumer Internet of Things

  Diese Spezifikation des Europäischen Instituts für Telekommunikationsnormen (ETSI) befasst sich insbesondere mit der Datensicherheit von vernetzten Geräten des IoT im Verbraucherbereich. Auch Themen des Datenschutzes werden hier adressiert.

- **DIN SPEC 27072**: Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit

Wie die ETSI TS 103 645 formuliert auch die DIN SPEC 27072 Mindestanforderungen an vernetzte Geräte bezüglich der Datensicherheit wie auch des Datenschutzes.

- **ISO/AWI 31700**: Consumer Protection — Privacy by Design for Consumer Goods and Services

  Der Ausschuss ISO/PC 317 entwickelt derzeit diese Norm, bei der das Thema Datenschutz bei vernetzten Konsumgeräten im Mittelpunkt steht. Über die einzelnen Inhalte ist derzeit noch wenig Konkretes bekannt.

- **DIN EN ISO/IEC 27001:** Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen
  und
  DIN EN ISO/IEC 27002: Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen:

  Bei diesen beiden Normen handelt es sich um Managementnormen für die Gestaltung sicherer Prozesse im Umgang mit Daten in Organisationen.

- **Verordnungen von EU-Richtlinien oder Gesetze**

  Neben Normen und Spezifikationen regeln auch manche Durchführungsverordnungen von EU-Richtlinien oder Gesetze auf nationaler Ebene schon spezifisch die speziellen Abläufe von Prozessen oder Höchst- bzw. Mindestwerte. Hier wurden

  - das „Gesetz zur Kennzeichnung von energieverbrauchsrelevanten Produkten, Kraftfahrzeugen und Reifen mit Angaben über den Verbrauch an Energie und an anderen wichtigen Ressourcen“ (EnVKG),
  - das „Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten“ (ElektroG) und
  - die „Verordnung […] im Hinblick auf die Festlegung von Ökodesign-Anforderungen an den Stromverbrauch elektrischer und elektronischer Haushalts- und Bürogeräte im Bereitschafts- und im Aus-Zustand sowie im vernetzten Bereitschaftsbetrieb“ der Ökodesign-Richtlinie

  auf Inhalte und Festlegungen untersucht.

4.2. Abgleich von Verbraucheranforderungen und Normen

Die in Kapitel 4.1 identifizierten Normen und Spezifikationen wurden daraufhin untersucht, ob sie bestimmte Verbraucheranforderungen – oder zumindest Teile der Anforderungen – bereits beinhalten. Die Ergebnisse dieses Abgleichs wurden im Fachgespräch vorgestellt und mit den Expertinnen und Experten diskutiert. Die

finalen Erkenntnisse werden im Folgenden für jede Verbraucheranforderung einzeln und erneut nach Leitwerten geordnet vorgestellt.

4.2.1. Leitwert 1: Sicherheit und gesundheitliche Unversehrtheit der Verbraucher

VA1: Von „smarten“ Spielzeugen darf keine Gefahr durch elektrische Schläge, elektromagnetische Strahlung oder selbständigen Bewegungen des Spielzeugs ausgehen. Zudem dürfen durch Bildschirme keine Sehstörungen bei Kindern entstehen und es bedarf Höchstwerten bezüglich der Geräuschbelastung.

Die DIN EN 62115 befasst sich mit elektrischer Sicherheit, elektromagnetischer (optischer) Strahlung und der Sicherheit bei elektrischen Fehlfunktionen.[73] Die DIN EN 71-1 regelt zudem Geräuschobergrenzen.[74] Die Normen DIN EN ISO 9241-303 beschreibt Anforderungen an elektronische optische Anzeigen.[75] Diese Verbraucheranforderung wird also zu großen Teilen schon in Normen und Spezifikationen adressiert.

VA2: Eine unbefugte Kontaktaufnahme durch Dritte und Manipulation der Kinder über einen unerlaubten Fernzugriff, die zu einer physischen oder psychischen Schädigung führen kann, muss ausgeschlossen sein.

In DIN EN 62115 wird auf die Sicherheit von Fernbedienungen für elektrisches Fahrspielzeug eingegangen.[76] Die Norm beinhaltet Anforderungen zur Verringerung von Sicherheitsrisiken, die sich aus dem Verlust der Fernsteuerung von elektrischem Aufsitzspielzeug ergeben. Diese sind jedoch sehr spezifisch und beziehen sich nicht direkt auf „vernetzte“ Spielzeuge. Derzeit wird diese Verbraucheranforderung somit noch nicht in der Spielzeugnorm DIN EN 62115 adressiert. Die Sicherheit von Datenübertragungen (siehe VA9) kann jedoch als Voraussetzung für die Erfüllung dieser Verbraucheranforderung begriffen werden und wird sowohl durch ETSI TS 103 645 als auch die DIN SPEC 27072 gefordert. Somit wird auch diese Verbraucheranforderung dort bereits adressiert.

4.2.2. Leitwert 2: Datenschutz und Datensicherheit, sowie Schutz der Persönlichkeitsrechte

VA3: Die Verbindung von „smarten“ Spielzeugen zum Internet und anderen Geräten sollte einfach zu beenden sein.

[73] DIN EN 62115: Elektrische Spielzeuge – Sicherheit
[74] DIN EN 71-1: Sicherheit von Spielzeug – Mechanische und physikalische Eigenschaften
[75] DIN EN ISO 9241-303: Ergonomie der Mensch-System-Interaktion – Teil 303: Anforderungen an elektronische optische Anzeigen.
[76] DIN EN 62115: Elektrische Spielzeuge – Sicherheit

Die Verordnung der Ökodesign-Richtlinie zum Standby fordert, dass Nutzerinnen und Nutzer von vernetzten Geräten die Möglichkeit haben müssen, drahtlose Netzwerkverbindungen zu deaktivieren.[77] Diese Anforderung gilt nicht für Produkte, die ausschließlich für die Nutzung über eine einzige drahtlose Netzwerkverbindung bestimmt sind. Zudem wird in der Verordnung nicht auf die Verbindung zwischen dem „smarten“ Spielzeug und der Steuerungs-App eines vernetzten Geräts (z.B. Smartphone) eingegangen. Da auch über die App mittelbar die Daten des „smarten“ Spielzeugs an einen externen Server gesendet werden können, sollte auch dieser Fall noch in einer Norm adressiert werden. Insofern bedarf es hier einer weiteren Konkretisierung und Spezifizierung für „smarte“ Spielzeuge.

VA4: Die Einstellung zur Datennutzung bei „smarten“ Spielzeugen sollten möglichst nutzerfreundlich ausgestaltet und datensparsam sein. Dazu müssen die DSGVO-Prinzipien des Privacy by design und Privacy by default berücksichtigt und verbraucherfreundlich ausgelegt werden.

Laut ETSI TS 103 645 bedeutet „die Einholung der Einwilligung „in gültiger Weise“ […] in der Regel, dass die Verbraucher die freie, offensichtliche und ausdrückliche opt-in Wahl haben, ob ihre personenbezogenen Daten für einen bestimmten Zweck verwendet werden dürfen.“[78] Die derzeit in der Entwicklung befindliche ISO 31700 wird ebenfalls bestimmte Anforderungen für eine adäquate Umsetzung von Privacy by design formulieren.[79] Diese Verbraucheranforderung wird somit bereits adressiert.

VA5: Bei der Inbetriebnahme smarter Spielzeuge sowie bei Updates und sonstigen Veränderungen müssen die Eltern ausdrücklich der Datenübertragung und -nutzung zustimmen. Dabei muss eine informierte, differenzierte, freiwillige und widerrufbare Einwilligung ermöglicht werden.

Neben dem zuvor genannten Passus zur Einwilligung und opt-in, fordert die ETSI TS 103 645 auch, dass die „Zustimmung in gültiger Weise einzuholen“ ist, falls „personenbezogene Daten auf der Grundlage der Zustimmung der Verbraucher verarbeitet werden. Den Verbrauchern, die der Verarbeitung ihrer personenbezogenen Daten zugestimmt haben, wird die Möglichkeit gegeben, diese jederzeit zu widerrufen.“[80] Lediglich die Möglichkeit der Differenzierung

---

[77] Umweltbundesamt (2013). Ökodesign- Richtlinie. Abgerufen von: https://www.umweltbundesamt.de/sites/default/files/medien/376/dokumente/datenblatt_oekodesign-richtlinie_standby-_und_schein-aus-_off-mode-verluste_und_verluste_im_vernetzten_bereitschaftsbetrieb.pdf (21.10.2019).

[78] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

[79] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).

[80] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

bei der Einwilligung wird hier noch nicht gefordert. Bei der ISO 31700 sind ebenfalls Inhalte zur Einwilligung zu erwarten. Die meisten Aspekte dieser Verbraucheranforderung sind somit schon in verschiedenen Normen und Spezifikationen formuliert.

VA6: Eine Aufnahme per Mikrophon oder Kamera darf nur nach bewusstem Befehl durch die Nutzerinnen und Nutzer erfolgen. Zudem muss immer deutlich erkennbar sein, wenn „smarte“ Spielzeuge Daten aufnehmen. Diese Anforderung gilt auch für Apps von Drittanbietern zur Steuerung von „smarten“ Spielzeugen.

Hier gibt es noch keine konkreten Normen oder Standards. Der §90 Absatz 1 des Telekommunikationsgesetztes definiert lediglich in negativer Weise, wie Geräte nicht beschaffen sein dürfen, da sie ansonsten als verbotene Sendeanlage gelten. Eine wichtige Unterscheidung ist hierbei, ob die von einem „smarten“ Spielzeug aufgenommenen Bild- oder Audiodateien nur lokal gespeichert werden, oder ob eine kabellose Übertragung von Bild- oder Audiodateien vorliegt. Werden Aufnahmen nur lokal gespeichert, handelt es sich nicht um eine Sendeanlage, sodass § 90 Abs. 1 TKG nicht gilt. Eine Norm oder Spezifikation mit einer positiven Formulierung wie „smarte“ Spielzeuge beschaffen sein müssen, um gesetzeskonform zu sein, wäre wünschenswert. Bei der Formulierung einer solchen Norm sollte genau definiert werden, wann eine Aufzeichnung „deutlich erkennbar“ ist und was unter „bewussten Befehlen“ verstanden wird. Dazu kann auf die Prüfkriterien der Bundesnetzagentur hinsichtlich eines Verstoßes gegen § 90 Abs. 1 TKG zurückgegriffen werden. Diese hat beispielsweise bestimmte Maßnahmen – wie den Einsatz von Signalwörtern oder von Tastendruckverfahren – als ausreichend für eine bewusste Aufzeichnung anerkannt.[81] Möglicherweise befasst sich auch die ISO 31700 mit diesen Aspekten. Hier gibt es also vielversprechende Ansatzpunkte, jedoch noch keine Norm oder Spezifikation, die diese Anforderung aufgreift.

VA7: Bei „smarten“ Spielzeugen ist sicherzustellen, dass die Datenschutzeinstellungen nur von den Eltern und nicht von den Kindern geändert werden können.

Die ISO 31700 soll laut dem Consumer & Public Interest Network (CPIN) der britischen Normungsbehörde BSI Vorgaben zu Privacy by design machen, die der realen Nutzung von Produkten und Dienstleistungen durch die Verbraucher entsprechen.[82] Insofern könnte diese Norm eventuell den Aspekt der „Kindersicherung“ bei „smarten“ Spielzeugen umfassen. Die Forderung konnte jedoch bislang in keiner Norm identifiziert werden.

VA8: Die Eltern müssen Informationen über die Speicherung sowie eine mögliche Weitergabe der Nutzer- und Nutzungsdaten einfach und schnell ermitteln sowie

[81] Darauf wurde in einem Schreiben der Bundesnetzagentur vom 18.07.2019 hingewiesen.
[82] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).

die gespeicherten Daten selbst verwalten und löschen können („Recht auf vergessen werden“). Dies gilt sowohl für lokal auf dem „smarten“ Spielzeug gespeicherte Daten als auch auf externen Servern.

Die ETSI TS 103 645 fordert eine einfache und schnelle Löschung von Nutzerdaten.[83] Zudem fordert die DIN SPEC 27072 die Möglichkeit der Löschung der erhobenen Nutzerdaten sowie eine Herstellung des Ausgangszustands.[84] Möglicherweise befasst sich auch die ISO 31700 mit diesem Aspekt. Somit werden viele Aspekte dieser Verbraucheranforderung bereits in Normen und Spezifikationen abgedeckt.

VA9: „Smarte“ Spielzeuge sollten eine sichere, verschlüsselte Verbindung bzw. Datenübertragung zum Internet sowie Drittgeräten aufweisen.

Sowohl die ETSI TS 103 645 als auch die DIN SPEC 27072 fordern eine sichere Verschlüsselung von Verbindungen zur Datenübertagung. Die DIN SPEC 27072 fordert bei der Kryptographie die Einhaltung des Stands der Technik[85], während die ETSI TS 103 645 eine Verschlüsselung fordert, die den Eigenschaften der Technologie und der Nutzung angemessen ist.[86] Diese Verbraucheranforderung ist somit bereits ausreichend adressiert.

VA10: „Smarte“ Spielzeuge sollten über adäquate, sichere Authentifizierungsmechanismen verfügen. Die Spielzeuge bzw. die zugehörigen Apps sollten immer per Default mit einem Passwort gesichert sein und dieses sollte hinreichend komplex sein.

Auch hier gibt es sowohl in der DIN SPEC 27072 als auch der ETSI TS 103 645 konkrete Vorgaben. Nach DIN SPEC 27072 müssen „bei der Inbetriebnahme des IoT-Geräts Standardpassworte für die Authentisierung […] individualisiert werden“.[87] Die ETSI TS 103 645 fordert, dass „alle IoT-Gerätepasswörter eindeutig sein müssen und nicht auf eine universelle Werkseinstellungswert zurückgesetzt werden können dürfen.“[88] Im Rahmen der ISO 31700 könnten zudem Anforderungen an die Art der Authentifizierung formuliert werden, da die Vorgaben „der realen Nutzung von Produkten und Dienstleistungen durch die

[83] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).
[84] DIN SPEC 27072: Mehr Sicherheit im Smart Home.
[85] DIN SPEC 27072: Mehr Sicherheit im Smart Home.
[86] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).
[87] DIN SPEC 27072: Mehr Sicherheit im Smart Home.
[88] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

Verbraucher entsprechen“ sollen.[89] Es bestehen somit Konkretisierungen für diese Verbraucheranforderung in verschiedenen Normen und Spezifikationen.

VA11: Security by design sollte bei der Entwicklung der Spielzeuge berücksichtigt werden. Unter anderem sollte das Betriebssystem von „smarten“ Spielzeugen immer nur so komplex wie nötig sein, da sonst unnötige Sicherheitslücken entstehen können („Minimalprinzip“).

Die ETSI TS 103 645 adressiert verschiedene Prinzipien des Security by design etwa durch das „principle of least privilege“. Demnach sollten unter anderem ungenutzte Software deaktiviert und ungenutzte Ports geschlossen sein. Der zugrundeliegende Code für die Software sollte zudem auf die notwendigen Funktionen beschränkt sein.[90] Es gibt somit bereits konkrete Anweisungen bezüglich dieser Verbraucheranforderung in dieser Spezifikation.

VA12: Auch sollten die Sicherheitseinstellungen so voreingestellt sein, dass Risiken minimiert sind (security by default).

Verschiedene Aspekte des security by default sind in der DIN SPEC 27072 vermerkt. So müssen beispielsweise alle Funktionen für die Online-Nutzung, die nicht für die Inbetriebnahme des IoT-Gerätes notwendig sind, deaktiviert sein.[91] Zudem wird empfohlen, dass die automatische Installation von Sicherheitsupdates standardmäßig aktiviert ist. Die Verbraucheranforderung wird also bereits in dieser Spezifikation adressiert, wobei die Benennung weiterer Voreinstellungen, die benutzerfreundlich gestaltet sein müssen, folgen sollte.

VA13: Für „smarte“ Spielzeuge müssen Sicherheitsupdates zur Verfügung gestellt werden, um die langfristige Sicherheit zu garantieren. Diese Pflicht besteht so lange Verbraucher dies „vernünftigerweise“ erwarten können. Hierfür müssen die Hersteller den Markt und ihre Produkte und Dienstleistungen regelmäßig auf Sicherheitslücken hin überprüfen.

Während die DIN SPEC 27072 empfiehlt, dass automatische Sicherheitsupdates standardmäßig eingestellt sind, stellt die ETSI TS 103 645 eine Liste an Anforderungen an Sicherheitsupdates von vernetzen Geräten bereit.[92] Unter anderem wird gefordert, dass alle Softwarekomponenten sicher aktualisierbar sein sollten und dass die Hersteller über bereitstehende Sicherheitsupdates informieren. Im Rahmen der ISO 31700 sollen zudem Anforderungen festgeschrieben werden, damit die Sicherheit eines vernetzten Geräts während der gesamten Lebensdauer überwacht und aufrechterhalten wird. Dies könnte

[89] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).
[90] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).
[91] DIN SPEC 27072: Mehr Sicherheit im Smart Home.
[92] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

auch die Bereitstellung von Sicherheitsupdates in angemessener Weise beinhalten.[93] Aspekte zu dieser Verbraucheranforderung sind also bereits in verschiedenen Normen und Spezifikationen enthalten.

VA14: Neben einer ausreichenden Sicherung der Daten auf dem „smarten“ Spielzeug müssen auch externe Server, auf denen Daten der Kinder gespeichert oder verarbeitet werden, adäquat gegen Cyberangriffe und Datendiebstahl geschützt sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt Vorgaben für ein sicheres IT-Management nach ISO 27001 heraus.[94] So stellen der IT-Grundschutz, die BSI-Standards zur Internet-Sicherheit (ISi-Reihe) und der Anforderungskatalog Cloud Computing (C5) konkrete Informationen zu Vorgaben und Anforderungen an einen sicheren Aufbau und Betrieb von Servern – durch den Anbieter selbst oder durch Dritte – bereit. Normen für den sicheren Aufbau und Betrieb von Servern gibt es jedoch nicht. Die Forderung, dass die Sicherheit von externen Servern gewährleistet sein muss, ist somit nur teilweise erfüllt.

4.2.3. Leitwert 3: Verhindern ökonomischer Nachteile für Verbraucher

VA15: Es muss sichergestellt werden, dass keine Lock-in-Effekte entstehen. Dazu muss die Datenportabilität zwischen vergleichbaren „smarten“ Spielzeugen gewährleistet sein. Auch eine Interoperabilität mit anderen vernetzten Geräten sollte möglich sein, wofür einheitliche Standards notwendig sind.

Zum Umgang mit Datenportabilität und Interoperabilität konnten keine Vorgaben in den analysierten Normen und Spezifikationen identifiziert werden.

VA16: Die Kinder als Nutzer sollten vor (versteckten) Kosten durch In-App-Käufe geschützt werden (z.B. durch erneute Authentifizierung durch die Eltern vor In-App-Käufen).

Hier könnten im Rahmen der ISO 31700 entsprechende Anforderungen formuliert werden, da die Vorgaben „der realen Nutzung von Produkten und Dienstleistungen durch die Verbraucher entsprechen“ sollen.[95] Dies wäre bei Kindern als Nutzern von „smarten“ Spielzeugen ein wichtiger Aspekt. Bisher konnten zur Verhinderung von In-App-Käufen durch Kinder keine Vorgaben in Normen und Spezifikationen identifiziert werden.

---

[93] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).

[94] Bundesamt für Sicherheit und Informationstechnik (2019). IT-Grundschutz-Kompendium – Edition 2019. Abgerufen von: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html;jsessionid=E8C21024C9D86185D498F29C8B8BC7AB.2_cid369 (21.10.2019).

[95] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).

VA17: Die Kinder sollten vor der Nutzung ihrer Daten zu Marketingzwecken geschützt werden. Das Geschäftsmodell „Daten gegen Leistung“ sollte bei „smarten“ Spielzeugen nur bei Einwilligung der Erziehungsberechtigten möglich sein.

Auch hier könnten im Rahmen der ISO 31700 entsprechende Anforderungen formuliert werden.[96] Zur Nutzung der Daten von Kindern zu Marketingzwecken und einer Notwendigkeit der Einwilligung der Eltern konnten bisher allerdings keine Vorgaben in Normen und Spezifikationen identifiziert werden.

4.2.4. Leitwert 4: Gebrauchstauglichkeit und Qualität von Produkten und Dienstleistungen

VA18: Gewährleistungsansprüche für „smarte“ Spielzeuge sollten auch für alle zugehörigen Dienstleistungen gelten, die für die Nutzung des „smarten“ Spielzeugs benötigt werden.

Zu Gewährleistungsansprüchen für zugehörige Dienstleistungen konnten keine Vorgaben in Normen und Spezifikationen identifiziert werden.

VA19: Gewährleistungsansprüche müssen auch dann gelten, wenn Verbraucher digitale Güter nicht mit Geld bezahlen, sondern im Gegenzug für ihre Daten erhalten.

Zu Gewährleistungsansprüchen bei der Bezahlung mit Daten konnten keine Vorgaben in Normen und Spezifikationen identifiziert werden.

VA20: Produkt-Updates sollten optional angeboten werden, falls sie nicht sicherheitsrelevant sind. Auch müssen die Geräte „updatefähig“ sein und die Installation der Updates für die Nutzer muss einfach gestaltet sowie ohne technisches Wissen durchführbar sein.

Bei dieser Verbraucheranforderung werden in der DIN SPEC 27072 und der ETSI TS 103 645 die Themen der Updatefähigkeit und Durchführung der Installation adressiert. So verlangt die ETSI TS 103645, dass alle Softwarekomponenten sicher aktualisierbar sein sollten, dass die Notwendigkeit jeder Aktualisierung deutlich gemacht wird und dass Updates einfach zu implementieren sein sollten.[97] Die DIN SPEC 27072 fordert, dass „das IoT-Gerät […] über einen Update-Mechanismus für die Installation von Software-Updates verfügen muss.“ Da sich jedoch beide Spezifikationen vor allem auf Sicherheitsupdates beziehen, wird auf das optionale Anbieten von Produkt-Updates nicht eingegangen und eine weitere Konkretisierung ist hier wohl erforderlich.

---

[96] Consumer and Public Interest Network (o.D.). Protecting consumers from harm in the digital market. Abgerufen von: https://www.bsigroup.com/globalassets/documents/s19038_bsi_cpin-brochure---digital_web.pdf (21.10.2019).

[97] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

VA21: Elektronische Verschleißteile wie Batterien, Akkus und Displays sollten möglichst einfach ausgetauscht werden können, aber gleichzeitig für die Kinder nicht erreichbar sein (Batterien und Akkus) bzw. „Kinderfest“ (Displays) sein.

Die DIN EN 62115 beinhaltet Anweisungen zum Umgang mit Batterien und Akkus. Allerdings steht hier die Sicherheit der Kinder im Vordergrund und dass diese die Batterien und Akkus nicht erreichen können. Bezüglich Bildschirmen beschreibt die Norm DIN EN ISO 9241 303 Anforderungen an elektronische optische Anzeigen, allerdings wird nicht auf den Austausch von Bildschirmen eingegangen.[98] Eine weitere Überarbeitung und Konkretisierung für „smarte“ Spielzeuge der bestehenden Normen scheint hier wohl notwendig.

VA22: Hersteller sollten darauf achten, dass die „smarten“ Spielzeuge barrierefrei zu bedienen sind. Dies gilt insbesondere auch für die Nutzung durch Kinder mit Behinderungen oder anderen Einschränkungen.

Zu einem barrierefreien Gebrauch durch Kinder mit Einschränkungen konnten keine Vorgaben in Normen und Spezifikationen identifiziert werden.

4.2.5. Leitwert 5: Prinzipien der Nachhaltigkeit

VA23: Die Hersteller müssen in der Produktinformation die Energieeffizienz kennzeichnen und mit den Produkten Leitlinien für eine effiziente Nutzung und Entsorgung von „smarten“ Spielzeugen bereitstellen.

Die Kennzeichnung der Energieeffizienz ist im Gesetz zur Kennzeichnung von energieverbrauchsrelevanten Produkten, Kraftfahrzeugen und Reifen mit Angaben über den Verbrauch an Energie und an anderen wichtigen Ressourcen (EnVKG) geregelt.[99] Auch wenn sie hier nicht explizit erwähnt werden, so fallen hierunter auch „smarte“ Spielzeuge. Das Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten (ElektroG) regelt in § 28 die Informationspflichten der Hersteller zur Entsorgung von Batterien.[100] Es gilt ausdrücklich für „elektrisches und elektronisches“ Spielzeug und umfasst somit auch „smarte“ Spielzeuge. Wie diese gesetzlichen Vorgaben konkret umgesetzt werden sollten, könnte zudem in Normen noch weiter spezifiziert werden.

VA24: „Smarte“ Spielzeuge müssen so konstruiert sein, dass sie in bestimmten, wenig genutzten Zeiträumen automatisch Energie sparen. Dies sollte schon in den Werkseinstellungen berücksichtigt werden (Energiesparsamkeit by Default).

---

[98] DIN EN ISO 9241-303: Ergonomie der Mensch-System-Interaktion – Teil 303: Anforderungen an elektronische optische Anzeigen.

[99] Gesetz zur Kennzeichnung von energieverbrauchsrelevanten Produkten, Kraftfahrzeugen und Reifen mit Angaben über den Verbrauch an Energie und an anderen wichtigen Ressourcen (Energieverbrauchskennzeichnungsgesetz – EnVKG) Abgerufen von: https://www.gesetze-im-internet.de/envkg_2012/BJNR107010012.html (21.10.2019).

[100] Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten (Elektro- und Elektronikgesetz- ElektroG) Abgerufen von: https://www.gesetze-im-internet.de/elektrog_2015/BJNR173910015.html#BJNR173910015BJNG000100000 (21.10.2019).

Die Verordnung der Ökodesignrichtlinie zum Standby-Modus ist sehr konkret und gibt Regeln und Grenzwerte zum Stromverbrauch im Aus-Zustand und Standby-Zustand vor.[101] Somit ist diese Verbraucheranforderung durch diese Verordnung abdeckt.

4.2.6. Leitwert 6: Herstellung von Transparenz und Vergleichbarkeit auf Märkten

VA25: Die Nutzungsbestimmung und die Regelungen zur Verarbeitung und Weitergabe von Daten sollten einfach zugänglich und transparent gestaltet sein. Zudem würden maschinenauslesbare Datenschutzerklärungen die Vergleichbarkeit für die Verbraucherinnen und Verbraucher erhöhen.

Die ETSI TS 103 645 fordert, dass den Nutzerinnen und Nutzern klare und transparente Informationen über die Verwendung und Verarbeitung personenbezogener Daten zur Verfügung gestellt werden müssen.[102] Dies gilt für jedes Gerät und jeden Dienst. Auch über die Zwecke, wie z.B. personalisierte Werbung, muss informiert werden. Insofern sind die meisten Aspekte dieser Verbraucheranforderung abgedeckt, eine Forderung nach maschinenauslesbaren Datenschutzerklärungen konnte allerdings bisher in keiner Norm oder Spezifikation identifiziert werden.

VA26: Die Anbieter von „smarten“ Spielzeugen sollten verpflichtend kennzeichnen müssen, wenn sie algorithmische Systeme nutzen und über deren Funktionsweise aufklären.

Zur Kennzeichnung künstlicher Intelligenz von vernetzten Geräten allgemein oder spezifisch von „smarten“ Spielzeugen konnten keine Anforderungen in den untersuchten Normen gefunden werden.

VA27: Relevante vorvertragliche Informationen sollten vergleichbar und transparent dargestellt werden. Dies betrifft etwa die erwartete Dauer der Updatebereitstellung, die Reparaturfähigkeit, die Energieeffizienz sowie die Notwendigkeit von Apps oder zusätzlichen Dienstleistungen für die Nutzung.

Sowohl die ETSI TS 103 645 als auch die DIN SPEC 27072 beschreiben eine Praxis zur Bereitstellung von Informationen zur Software-Update-Policy.[103] Zu vorvertraglichen Informationen über die Energieeffizienz greift hier wieder das EnVKG. Zu Informationen bezüglich der Reparaturfähigkeit, über zusätzliche Dienste oder die Notwendigkeit von Apps konnten keine Vorgaben in Normen

---

[101] Umweltbundesamt (2013). Ökodesign-Richtlinie. Abgerufen von: https://www.umweltbundesamt.de/sites/default/files/medien/376/dokumente/datenblatt_oekodesign-richtlinie_standby-_und_schein-aus-_off-mode-verluste_und_verluste_im_vernetzten_bereitschaftsbetrieb.pdf (21.10.2019).

[102] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019).

[103] ETSI TS 103645: Cyber Security for Consumer Internet of Things. Abgerufen von: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (21.10.2019) und
DIN SPEC 27072: Mehr Sicherheit im Smart Home.

und Spezifikationen identifiziert werden. Somit sind verschiedene Aspekte bereits in Normen und Spezifikationen abgedeckt, während bei anderen noch Konkretisierungsbedarf besteht.

4.2.7. Leitwert 8: Interessen besonders schutzbedürftiger gesellschaftlicher Gruppen

VA28: Die Anbieter von Dienstleistungen für „smarte“ Spielzeuge, die Chatfunktionen umfassen, müssen sicherstellen, dass keine jugendgefährdenden Inhalte über diese Chatfunktion geteilt und verbreitet werden. Eine Lösung hierfür ist eine professionelle Moderation des Chats.

Zum Umgang mit jugendgefährdenden Inhalten in Chats konnten keine Normen und Spezifikationen identifiziert werden.

4.2.8. Zwischenfazit zum Abgleich der Verbraucheranforderungen mit Normen und Spezifikationen

Um einen **Überblick** über die Ergebnisse des vierten Kapitels zu geben, stellt **Tabelle 2** für die einzelnen Verbraucheranforderungen schematisch dar, inwiefern die Verbraucheranforderungen schon in bestehenden, relevanten Normen und Spezifikationen adressiert und umgesetzt sind. Dabei wird zwischen Umsetzungsstadien von Verbraucheranforderungen unterschieden: Verbraucheranforderungen, die schon größtenteils in der Norm oder Spezifikation adressiert sind (dunkelgrün); Verbraucheranforderungen, die zumindest teilweise in der Norm oder Spezifikation adressiert sind (hellgrün); und Verbraucheranforderungen, die noch gar nicht in der Norm oder Spezifikation adressiert sind (farblos). Insgesamt wird deutlich, dass bezüglich der Umsetzung von Verbraucheranforderungen an „smartes“ Spielzeug in Normen und Spezifikationen derzeit ein heterogenes Bild besteht:

So werden bereits viele Aspekte der ersten beiden Leitwerte (**physische Sicherheit, Datensicherheit und Datenschutz**) in Normen und Spezifikationen beschrieben oder sind Gegenstand laufender Normungsprozesse – wie im Falle der ISO 31700. Allerdings gibt es auch hier noch Bedarf an weiteren Konkretisierungen, z.B. bei der Kennzeichnung von und Einwilligung zu Aufnahmen. Auch bezüglich Verbraucheranforderungen, die sich spezifisch an „smarte“ Spielzeuge mit Kindern als Zielgruppe richten – wie etwa eine „Kindersicherung“ bei den Datenschutzeinstellungen – gibt es noch keine Normen und Spezifikationen.

Die zur **Verhinderung ökonomischer Nachteile** identifizierten Verbraucheranforderungen von Leitwert 3 wurden bisher noch nicht in den hier untersuchten Normen festgelegt und es bleibt abzuwarten, inwiefern die ISO 31700 dieses Thema – insbesondere bei In-App-Käufen – adressieren wird.

Beim vierten Leitwert (**Gebrauchstauglichkeit und Qualität von Produkten und Dienstleistungen**) besteht insbesondere bei der Anpassung von Gewährleistungsansprüchen an die digitale Welt noch Handlungsbedarf.

Für die Verbraucheranforderungen von Leitwert 5 (**Prinzipien der Nachhaltigkeit**) sind vor allem gesetzliche Regelungen und Vorgaben relevant. Hier werden die meisten Anforderungen schon explizit geregelt, eine weitere Konkretisierung – d.h. eine Anleitung zur Einhaltung dieser Anforderungen – in Normen könnte aber sehr hilfreich sein.

Abgesehen von vorvertraglichen Informationen zum Einsatz künstlicher Intelligenz und dem möglichen Zwang zum Kauf von Zusatzleistungen werden auch die Verbraucheranforderungen des sechsten Leitwerts (**Herstellung von Transparenz und Vergleichbarkeit auf Märkten**) schon in Normen und Spezifikationen gefordert.

Die Anforderung an eine Regulierung möglicher Chat-Funktionen von „smarten“ Spielzeugen des achten Leitwerts (**Interessen besonders schutzbedürftiger gesellschaftlicher Gruppen**), ist bisher noch nicht in Normen und Spezifikationen beschrieben.

Leitwerte	VAs	DIN EN 71	DIN EN 62115	ETSI TS 103 645	DIN SPEC 27072	ISO 31700	ISO 27001/27002	EnVKG	ElektroG	Ökodesign-Richtlinie
1) Physische und psychische Sicherheit	VA1									
	VA2									
2) Datenschutz	VA3									
	VA4									
	VA5									
	VA6									
	VA7									
	VA8									
2) Datensicherheit	VA9									
	VA10									
	VA11									
	VA12									
	VA13									
	VA14									
3) Verhindern ökonomischer Nachteile	VA15									
	VA16									
	VA17									
4) Gebrauchstauglichkeit und Qualität	VA18									
	VA19									
	VA20									
	VA21									
	VA22									
5)Nachhaltigkeit	VA23									
	VA24									
6) Transparenz	VA25									
	VA26									
	VA27									
8) Schutzbedürftige Gruppen	VA28									

Tabelle 2: Abgleich von Verbraucheranforderungen mit Normen, Spezifikationen und gesetzlichen Spezifizierungen

Legende: Dunkelgrün=Verbraucheranforderungen Großteils erfüllt; Hellgrün= Verbraucheranforderungen teilweise oder möglicherweise bald erfüllt

5. Ableitung von Handlungsempfehlungen

Die Analyse zeigt, dass Verbraucheranforderungen an „smarte“ Spielzeuge grundsätzlich in zwei Typen eingeteilt werden können: allgemeine und Spielzeug-spezifische Verbraucheranforderungen. Dementsprechend gilt es auch verschiedene Institutionen bzw. Normungsausschüsse zu adressieren, wenn man die unterschiedlichen Verbraucheranforderungen in Normen und Spezifikationen umsetzen möchte. Denn einerseits gibt es Normen zu vernetzten Geräten, die in Normungsausschüssen zum Thema „Internet of Things“ ausgearbeitet werden, und andererseits spezifische Spielzeugnormen, die in Normungsausschüssen zum Thema Spielzeug verabschiedet werden. Dabei ist es bezüglich der allgemeinen Aspekte der Informationstechnik – wie etwa Datensicherheit oder Datenschutz – von Vorteil, wenn Querschnittsnormen zu vernetzten Geräten von Experten auf diesem Gebiet entwickelt werden – also in den Normungsgremien zum Thema „Internet of Things“. Auf die dort entwickelten Inhalte sollte dann in Spielzeugnormen verwiesen werden. Verbraucheranforderungen, die nur spezifisch für „smarte“ Spielzeuge gelten, sollten zudem in den Ausschüssen für Spielzeugnormung entwickelt und verabschiedet werden. Dazu müsste jedoch deren Zuständigkeitsbereich angepasst werden.

Da die verschiedenen Verbraucheranforderungen also in unterschiedlichen Normungsgremien bzw. Normen adressiert werden, bedarf es eines multidimensionalen Vorgehens: Einerseits sollten **Querschnittsnormen für vernetzte Geräte** adressiert werden **(Empfehlungen 1 und 2)**, andererseits sollten **spezifischere Inhalte in Spielzeugnormen (Empfehlung 3)** einfließen. Im Folgenden werden diese verschiedenen Ansatzpunkte vorgestellt und entsprechende Handlungsempfehlungen abgeleitet.

1.) Einbringen von Verbraucheranforderungen für vernetzte Geräte in die Norm ETSI EN 303 645

Aus den Spezifikationen ETSI TS 103 645 und der DIN SPEC 27072 entsteht derzeit eine neue europäische Norm, die ETSI EN 303 645 (Cyber Security for Consumer Internet of Things). Diese Norm adressiert insbesondere Aspekte der Datensicherheit von IoT-Produkten, teilweise aber auch die Ausgestaltung eines wirksamen Datenschutzes. Die Norm – bzw. der bei ETSI dafür zuständige Ausschuss **CYBER** – stellt also einen guten Ansatzpunkt dar, da 12 der 28 identifizierten Verbraucheranforderungen die Themen Datensicherheit und Datenschutz direkt betreffen (und zudem einige weitere Verbraucheranforderungen indirekt, wie etwa die Forderung nach Interoperabilität oder der Kennzeichnung künstlicher Intelligenz).

In Kapitel 4.2 wurde deutlich, dass beide Spezifikationen schon über bestimmte Inhalte zur Datensicherheit verfügen, die den Verbraucheranforderungen entsprechen. Deshalb ist zu erwarten, dass diese Inhalte auch in die finale Norm übernommen werden. Weitere Aspekte, die noch nicht ausreichend in einer der Spezi-

fikationen adressiert wurden – wie etwa die Benennung weiterer Datensicherheitsrelevanter Voreinstellungen (VA12) oder die Sicherheit von Servern (VA14) – sollten hier eingebracht werden.

Da die Entwicklung der Norm schon recht weit fortgeschritten ist und ein erster Entwurf schon Ende September 2019 verabschiedet wurde, könnte sich eine Einflussnahme zur Schließung der identifizierten Lücken hier allerdings schwierig gestalten. Es könnten jedoch Verbraucheranforderungen über ANEC im Rahmen der Kommentierung des Entwurfs eingebracht werden. Zudem übernimmt das BSI die Ausgestaltung der zugehörigen Testspezifikationen und kann dabei in einem gewissen Maße relevante Verbraucheranforderungen berücksichtigen.

2.) Vorschläge bei der Entwicklung der ISO 31700 zu Privacy by design einbringen

Während die Norm ETSI EN 303 645 vor allem die Datensicherheit adressieren wird, steht bei den Normungsarbeiten zur Norm ISO 31700 das Thema Privacy by design bei vernetzten Konsumgeräten und den zugehörigen Dienstleistungen – also der Datenschutz – im Mittelpunkt. Entsprechende Verbraucheranforderungen könnten im zuständigen Normungsausschuss **ISO/PC 317** eingebracht werden. Beispielhaft hierfür wäre eine konkrete Beschreibung von Methoden für eine deutlich erkennbare und bewusste Aufzeichnung (VA6) oder die Kennzeichnung des Einsatzes künstlicher Intelligenz (VA26).

Das relativ frühe Entwicklungsstadium des Normungsprozesses hat den Vorteil, dass noch viele Aspekte vorgeschlagen und eingebracht werden können. Gleichzeitig besteht aber somit auch die Gefahr, dass der Normungsprozess von bestimmten Stakeholdern dominiert wird und es deshalb schwierig werden kann bestimmte Inhalte einzubringen. Bei der ISO 31700 wird es sich zudem um eine internationale Norm handeln. Das hat den Vorteil, dass der geographische Gültigkeitsbereich größer sein wird als bei einer nationalen oder europäischen Norm. Allerdings dürfte das Sicherheitslevel niedriger als von deutscher Seite gewünscht ausfallen. Um auf der internationalen Ebene Einfluss zu nehmen, könnte der DIN-VR über ANEC an Consumers International herantreten oder über das nationale Spiegelgremium Änderungen vorschlagen.

3.) Erweiterung des Zuständigkeitsbereichs der DIN EN 62115 zur Bearbeitung spezifischer Verbraucheranforderungen an „smarte“ Spielzeuge

Zunächst liegt es nahe, dass spezifische Verbraucheranforderungen an „smarte“ Spielzeuge in der klassischen Spielzeugnormung bearbeitet bzw. in entsprechende Ausschüsse eingebracht werden könnten. Auf internationaler Ebene könnte also der Ausschuss **ISO/TC 181**, der für die ISO 8124-1 "Sicherheit von Spielzeug - Sicherheitsaspekte hinsichtlich mechanischer und physikalischer Eigenschaften“ (dem Äquivalent der deutschen DIN EN 71-1) zuständig ist, einen

Ansatzpunkt bieten. In diesem Ausschuss haben zudem schon die Vertreter Brasiliens und Großbritanniens in einer Umfrage die Bedeutung des Themas „smarte“ Spielzeuge signalisiert. Da in diesem Gremium der Einfluss der deutschen Vertreter jedoch begrenzt ist, stellt dies derzeit keine vorrangige Lösung dar.

Ein anderer, vielversprechenderer Ansatzpunkt ist die Norm IEC 62115 (Sicherheit von elektrischem Spielzeug, Äquivalent zu DIN EN 62115) bzw. das dafür zuständige internationale Normungsgremium **IEC/TC 61**. Hier könnten spezifische Verbraucheranforderungen an „smarte“ Spielzeuge eingebracht werden. Wie bei der Betrachtung der zweiten Verbraucheranforderung (Ausschluss einer unbefugten Kontaktaufnahme) deutlich wurde, umfasst die Norm aber nicht die Merkmale der drahtlosen Datenübertragung und somit noch nicht konkret „smarte“, vernetzte Spielzeuge. Deshalb müsste der Zuständigkeitsbereich der Norm und des Gremiums um elektronische und vernetzte Spielzeuge erweitert werden, damit die Bearbeitung relevanter Inhalte zu „smarten“, vernetzten Spielzeugen in diesem Gremium ermöglicht werden kann. Die IEC 62115 bzw. die DIN EN 62115 könnte dann grundsätzlich auf die Querschnittsnormen zu vernetzten Geräten (wie etwa der ETSI EN 303 645) verweisen, bestimme Besonderheiten und Abweichungen für „smarte“ Spielzeuge – wie etwa die „Kindersicherung“ bei den Datenschutzeinstellungen von „smarten“ Spielzeugen (VA7) – könnten hier spezifiziert werden. Für alle identifizierten Verbraucheranforderungen, die nicht durch bereits existierende Normen abgedeckt sind – wie etwa die Moderation von Chats zur Verhinderung jugendgefährdender Inhalte (VA28) –, könnte das IEC/TC 61 dann neue Normen entwickeln.

Um die Spielzeughersteller als relevante Stakeholder und in der Normung aktive Akteure für diese Idee zu gewinnen, sollten Maßnahmen zur Sensibilisierung umgesetzt werden. Dazu können – neben der Ansprache des Themas in den entsprechenden Normungsgremien – auch Vorträge oder Workshops zu „smarten Spielzeugen und Normung“ auf einschlägigen Veranstaltungen wie der Nürnberger Spielwarenmesse einen Beitrag leisten. In diesem Rahmen sollte auch über den Einbezug technischer Experten (z.B. vom TüV) für Vorträge nachgedacht werden.