



## DIN VR-Studie „Digitalisierungsaspekte und Verbrauchieranforderungen in Bezug auf smartes Spielzeug – Umsetzung in der Normung“

### Zielsetzung:

- Kategorisierung für smartes Spielzeug (App-gesteuerte und nicht IP-vernetzte Spielzeuge) erstellen
- Ermittlung von Verbrauchieranforderungen zu Digitalisierungsaspekten für smartes Spielzeug
- Ermittlung von Verbrauchieranforderungen zu Digitalisierungsaspekten auch für IoT (Internet- of-Things)
- Erarbeitung konkreter Vorschläge zu Verbrauchieranforderungen in Normen

### Allgemeine IoT-Verbrauchieranforderungen (VA) - Auszug

**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.

**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 sollten die DSGVO-Prinzipien des **Privacy by design** und **Privacy by default** berücksichtigt 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 sollte nur nach bewusstem Befehl durch die Nutzerinnen und Nutzer erfolgen. Zudem sollte immer deutlich erkennbar sein, wenn „smarte“ Spielzeuge Daten aufnehmen. Diese Anforderung gilt auch für Apps von Drittanbietern zur Steuerung von „smarten“ Spielzeugen.

**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.

**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.

**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).

### Übergeordnete Ergebnisse:

- „klassische“ Sicherheit von smartem Spielzeug weitgehend abgedeckt in DIN EN 71-1 „Sicherheit von Spielzeug - Mechanische und physikalische Eigenschaften“ und DIN EN 62115 „Elektrische Spielzeuge – Sicherheit“
- bereits gute Ansatzpunkte zu Datenschutz und Datensicherheit im IoT-Bereich
- Verhinderung ökonomischer Nachteile und Gebrauchstauglichkeit für Kinder
- 28 Verbrauchieranforderungen (VA) identifiziert, davon 7 spielzeugspezifische und 21 allgemeine IoT-Anforderungen

### spielzeugspezifische Verbrauchieranforderungen (VA)

**VA1:** Durch „smarte“ Spielzeuge dürfen keine Gefahr durch elektrische Schläge, elektromagnetische Strahlung oder selbständigen Bewegungen des Spielzeugs ausgeht. Zudem dürfen durch Bildschirme keine Sehstörungen bei Kindern entstehen und es bedarf Höchstwerten bezüglich der Geräuschbelastung.

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

**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.

**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.

**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.

**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.

### Handlungsempfehlungen:

- allgemeine Verbrauchieranforderungen verankern in ETSI EN 303 645 „Cyber Security for Consumer Internet of Things“ und ISO 31700 „Consumer Protection – Privacy by Design for consumer goods and services“
- spielzeugspezifische Verbrauchieranforderungen verankern in DIN EN 71-1 „Sicherheit von Spielzeug - Mechanische und physikalische Eigenschaften“ und DIN EN 62115 „Elektrische Spielzeuge – Sicherheit“

### Umsetzung in der Praxis

#### Erste Erfolge: Normen zu IoT-Produkten

- Erster Schritt in die richtige Richtung: ETSI EN 303 645 „Cyber Security for Consumer Internet of Things“ im Juni 2020 erstmalig veröffentlicht
- Rege Beteiligung des DIN-Verbraucherrates bei der Erarbeitung der Norm, verbraucherrelevante Aspekte größtenteils nur Empfehlungen, müssen im nächsten Schritt als Anforderungen festgelegt werden
- Noch in Erarbeitung: ISO 31700 „Consumer Protection – Privacy by Design for consumer goods and services“, DIN-Verbraucherrat bringt Verbrauchieranforderungen ein

#### Ungeklärt: Verbrauchieranforderungen zur digitalen Sicherheit in Spielzeugnormen

- Problem: EU-Spielzeugrichtlinie behandelt Sicherheit im Sinne von „safety“, nicht im Sinne von „security“
- Rückmeldung EU-Kommission: „Cyber Security“ auch in naher Zukunft **kein** Thema der EU-Spielzeugrichtlinie



© Viacheslav\_lakobchuk Fotolia.com

