

Mindestmaß an IT-Sicherheit bedenken!

Sie müssen kein IT-Profi sein, aber dass Passwörter nicht im Klartext beim Hersteller gespeichert werden und Kommunikation verschlüsselt sein sollte, ist selbsterklärend. Achten Sie auf solche und ähnliche Angaben beim Hersteller. Recherchieren Sie ggf. vorab im Netz.

Seriöse Hersteller sorgen gerne für Transparenz!

Profis informieren Sie über Sicherheitsmaßnahmen, z.B. in der Produktbeschreibung, den Datenschutzbestimmungen oder auf ihrer Internetseite. Ganz seriöse Hersteller prahlen aber nicht damit. Aufdringliche Versprechen wie „besonders sicher“ oder „100% DSGVO-konform“ sollten Sie mit Vorsicht genießen – zumal Werbeabteilungen Sie mit smarten Formulierungen ganz schön einlullen können.

Ziehen Sie Alternativen in Betracht!

Beispiel: Ein beliebtes Kinderspielzeug ist die „Toniebox“, die Musik und Hörbücher abspielen kann. Das Gerät sammelt viele Daten, die in einer Cloud gespeichert werden. Solch eine Box können Sie aber auch mit einem „Arduino“ [kleines Steuersystem] selbst bauen – ohne tiefgehende Programmierkenntnisse und ohne datensammelnde Hersteller im Nacken.

An die „großen Kinder“:

**Womit spielen Sie als Erwachsene?
Nutzen Sie ein smartes Fitnessarmband?
Freuen Sie sich über die Kaffeemaschine,
die sich über Ihre App bedienen lässt?**

Die Risiken bezüglich **Datenschutz** und **IT-Sicherheit** sind bei allen vernetzten Geräten hoch. Für Sie und Ihr Kind, denn es verlässt ja vermutlich nicht den Raum, wenn Sie die Sprachassistenten Siri [Apple] oder Alexa [Amazon] beschwören, um nach dem morgigen Wetter zu fragen. Letztere hört übrigens immer mit, nicht nur wenn Sie einen Sprachbefehl geben [zeichnet aber laut Hersteller nicht immer alles auf].

Datenschutz: Schutz von Menschen, ihrer personenbezogenen Daten, der Privatsphäre und informationeller Selbstbestimmung.

IT-Sicherheit: Schutz von Systemen, z.B. vor Fremdzugriff und Datenverlust.

Eine aktuelle Übersicht über verbotene Geräte und Spielzeuge finden Sie auf der Internetseite der Bundesnetzagentur:

[🔗bundesnetzagentur.de/DE/Vportal/TK/Produkte/start.html](https://www.bundesnetzagentur.de/DE/Vportal/TK/Produkte/start.html)

BESONDERHEIT VON KINDERDATEN

Die Daten von Erwachsenen sind für Unternehmen ein leichteres Ziel; denn Kinder bewegen sich erst mit steigendem Alter mehr im Netz, Verträge können ohnehin nur mit geschäftsfähigen Personen geschlossen werden, und die Daten von Kindern unterliegen grundsätzlich einem höheren Schutzniveau [das verlangen z.B. die UN-Kinderrechtskonvention und die DSGVO]. Das alles macht Kinderdaten besonders rar, aber auch besonders wertvoll. Es gibt immer mehr vernetzte Spielzeuge und Apps für Kinder,

aber auch zunehmend Software, die für schulische und außerschulische Bildung genutzt wird. Diese Angebote speziell für Kinder und Jugendliche bieten der Datenindustrie ganz neue Möglichkeiten, um über Hintertürchen an Daten dieser sensiblen Zielgruppe heranzukommen.

Kinder werden so immer früher zu „gläsernen“ Menschen. Ihre Interessen und Gewohnheiten

ermöglichen Analysen ihrer Persönlichkeit und ihres Charakters. Vor allem in jungen Jahren sind sie besonders lenk- und manipulierbar – und die Voraussage ihres Handelns ist Gold wert. Unternehmen nutzen diese wertvollen Informationen, z.B. um ihre eigenen Produkte zu optimieren und Umsätze zu steigern.

Artikel 16 der UN-Kinderrechtskonvention:

[1] Kein Kind darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. [2] Das Kind hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Erwägungsgrund 38 der DSGVO:

[1] Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. [2] Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. [...]

