Karin Tien und Jennifer Maria Held
Rechtsanwaltsanwärterinnen bei Knyrim Trieb Rechtsanwälte OG

Digitalisierung im Kinderzimmer: Rechtssicherer Umgang mit vernetztem Spielzeug und Internetspielen

Was muss nach der DSGVO beim Schutz von Daten Minderjähriger bei vernetzten Spielzeugen und Online-Spielen aus datenschutzrechtlicher Sicht beachtet werden? Die Spielwarenindustrie ist ein nicht zu unterschätzender Umschlagplatz für personenbezogene Daten von Spielern, die in vielen Fällen noch minderjährig sind. Der Grundsatz der Datenminimierung scheint für Anbieter im virtuellen Raum und im Kinderzimmer in den Hintergrund gerückt zu sein, der Fokus liegt meist auf der Monetarisierung der angebotenen Dienste auf Basis der Auswertung von Spielerdaten.

Einleitung und Problemaufriss

Die Digitalisierung macht auch vor den Kinderzimmertüren nicht halt, Kinder sind eine der interessantesten Zielgruppen der Spielwarenindustrie. Vernetzte Spielzeuge und Online-Spiele sammeln allerdings eine Vielzahl von personenbezogenen Daten. Dabei wird übersehen, dass deren Nutzung die Einwilligung der Eltern erfordern könnte. Mit Inkrafttreten der DSGVO[1]) und des (neuen) Datenschutzgesetzes (DSG[2]) am 25. 5. 2018 wird es Änderungen für Kinder, Eltern sowie Anbieter bei der Einholung von Einwilligungen geben.

§ 4 Abs 4 DSG statuiert, dass ein Minderjähriger, welcher das 14. Lebensjahr vollendet hat, nur bei einem direkten Angebot von Diensten der Informationsgesellschaft rechtmäßig in die Verarbeitung seiner Daten einwilligen kann, unterhalb dieser Altersgrenze kann die Einwilligung der Eltern als stellvertretend angesehen werden. Die Möglichkeit einer generellen Normierung einer datenschutzrechtlichen Regelung für Kinder und unmündige Minderjährige[3] haben die Gesetzgeber auf nationaler wie europäischer Ebene jedoch verabsäumt.

Wird die Systematik des § 170 ABGB konsequent auf das Datenschutzrecht angewandt, so würde dies dazu führen, dass Kinder in den meisten Fällen aufgrund mangelnder Einsichts- und Urteilsfähigkeit hinsichtlich des Umfangs und der Folgen der Datenverarbeitung keine rechtmäßige Einwilligung abgeben können.[4] Usus ist dabei geworden, die Einwilligung des Kindes durch die der Eltern zu substituieren, was aus rechtlicher Sicht zu hinterfragen ist (siehe weiter unten).

Online-Spiele

Online-Spiele sind für Kinder mittlerweile ein wesentlicher Teil ihrer sozialen Interaktion. Die Branche hat sich in den letzten Jahren deutlich fragmentiert und eine Vielzahl an Spielarten und Genres (wie Rollen- oder Simulationsspiele) hervorgebracht. Zudem werden technische Bestandteile der Hardware (bspw Neigungssensoren, GPS, Audio- und Videofunktionen) miteinbezogen und nutzen vermehrt Schnittstellen (wie Bluetooth).[5] Die Spiele unterscheiden sich zudem dadurch, auf welcher Plattform (Spielkonsolen, Browserspiele, Apps) sie gespielt werden können. Neben den klassischen Online-Spielen existieren Spiele, die eine Brücke zur „Offline"-Welt schlagen und Kindern die Möglichkeit bieten, das Online-Spielerlebnis mit physischen Handlungen zu kombinieren.[6] Zudem sind Weiterentwicklungen im Virtual Gaming Bereich zu erwarten, wie bspw das „Mimik- und Eye-Tracking", die insb bei Virtuellen Brillen zum Einsatz kommen.

Online-Spiele sammeln Informationen über den Spieler und sein Verhalten.

Während des Spieles werden Daten über den Spieler selbst oder über dessen Spielverhalten gesammelt; wobei dabei Rollenspiele hervorzuheben sind, die persönliche Wesensmerkmale (Analyse des sozialen Netzwerks, Häufigkeit der Kontaktaufnahme mit unbekannten Spielern) erfassen. Sofern die Verarbeitung der aus den Online-Spielen gewonnenen Daten nicht der Vertragserfüllung[7] dient, was bspw bei einer Auswertung der Kundenprofile der Fall wäre, ist die Einwilligung des Kindes bzw der Eltern erforderlich.[8]

Erfolgt die Nutzung der Daten des Online-Games auf Basis der Einwilligung eines Kindes,[9] so ist nach Art 8 DSGVO iVm § 170 ABGB auf dessen Einsichts- und Urteilsfähigkeit,[10] selbst bei Zustimmung durch die Eltern,[11] abzustellen. Demzufolge ist es für Eltern und Spieleanbieter gleichermaßen notwendig, altersgerecht eine Abstufung vorzunehmen, die sich an der Eingriffsintensität[12] und dem Geheimhaltungsinteresse des Kindes orientiert, sowie ebenso die Datenverarbeitung zur Eröffnung von Spieler-Konten und Spielerweiterungen[13] berücksichtigt.

„Smartes" Spielzeug

Unter dem Begriff „Connected Smart Toys" werden Spielzeuge[14] verstanden, welche mit

[1] VO (EU) 679/2016 des EP und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1. [2] BG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, BGBl I 2017/120. [3] Das österr Zivilrecht bezeichnet Personen als unmündig und somit eingeschränkt geschäftsfähig, welche das 14. Lebensjahr noch nicht vollendet haben, als Kinder Personen, welche die Altersgrenze von 7 Jahren noch nicht erreicht haben (§ 21 ABGB). [4] Luckos, Internet of Toys – Das vernetzte Spielzeug in datenschutzrechtlicher Sicht, MR 2017, 123. [5] Siehe dazu *Krieger-Lamina*, Privatsphäre in Online-Spielen. Spielend Daten sammeln, Bericht ITA 2017–04, http://epub.oeaw.ac.at/ita/ita-projektberichte/2017-04.pdf (Stand aller Links 10. 1. 2018). [6] Insb Augmented Reality Spiele wie Pokémon GO oder „Toys-to-Life Concept" mit Sammelfiguren (Nintendos Amiibo Figuren), die mit einem NFC-Chip versehen sind. [7] Art 6 Abs 1 lit b DSGVO. Für die Vertragserfüllung notwendige Daten sind einerseits die Kontaktdaten des Spielers (für das Erstellen eines Spielerprofils, Einhaltung Spielbedingungen, Nutzervertrag) und die technischen Daten der Hard-/Software (IP-Adresse, Browser-Typ und Zugriffszeiten). [8] *Pilgermair*, Datenschutz-Grundverordnung: Der neue Kinderschutz, Dako 2017/4. [9] Vgl *Erkeling*, Minderjährige als Vertragspartner eines Online-Game-Nutzungsvertrages, DSRITB 2016, 785. [10] Luckos, Internet of Toys – Das vernetzte Spielzeug in datenschutzrechtlicher Sicht, MR 2017, 123 (126). [11] *Rauda*, Gemeinsamkeiten von US Children Online Privacy Protection Act (COPPA) und DSGVO, MMR 2017, 17. [12] Insb Tragweite der Folgen der Datennutzung; eine erhöhte Eingriffsintensität kann bei sog „Massively Multiplayer Online Role Playing Games" im Gegensatz zu einem Online-Schachspiel angenommen werden. [13] Vgl *Leissler*, Intelligentes Spielzeug: Der Datenschutz im Kinderzimmer, ecolex 2017, 99 (100). [14] Smart Toys sind von den Herstellern meist für die Altersgruppe 3 bis 9 Jahre vorgesehen www.bmjv.de/SharedDocs/Downloads/DE/PDF/Berichte/Faktenblatt_Smartes-Spielzeug.pdf?__blob=publicationFile&v=1.

dem Spielenden oder anderen Geräten interagieren. Die „Connected Toys" besitzen die Fähigkeit, bspw. eigenständig Fragen zu stellen und machen sich die Möglichkeiten der Gesichts- und Spracherkennungstechnologien zu eigen.[15]

Vernetzte Spielzeuge übermitteln die Gespräche mit Kindern an eine Cloud.

Beispiel ist die Puppe „My friend Cayla", die ua eine Unterhaltung mit dem Kind führt.[16] Einzelne Wörter und Sätze des Betroffenen werden via App-Verbindung an die eigens dafür betriebene Cloud übermittelt, welche algorithmusbasiert eine Antwort generiert.[17] Es ist anzunehmen, dass Kinder während des Spielverlaufs ihren Smart Toys in einem Gespräch Daten über den eigenen Gesundheitszustand und weitere „sensible" Bereiche anvertrauen, weshalb die Übermittlung als durchaus kritisch zu betrachten ist. Ob das Kind nun eine Einwilligung als Rechtsgrundlage[18] für die Übermittlung besonderer Daten abgeben kann oder ob die Eltern dies stellvertretend tun können, gilt es in Zukunft zu klären.

Bislang kann angenommen werden, dass bei dem Recht auf Datenschutz als ein höchstpersönliches Recht in Bezug auf besondere Kategorien personenbezogener Daten[19] „Vertretungsfeindlichkeit" bestehen könnte. Wird die Systematik des § 170 ABGB, welche auf die Urteils- und Einsichtsfähigkeit der betreffenden Kinder und Jugendlichen abstellt und Altersgrenzen definiert, konsequent auf das Datenschutzrecht angewandt, bedeutet dies,[20] dass Eltern keine rechtmäßige Einwilligung stellvertretend abgeben können, wenn es sich um Daten handelt, welche den „höchstpersönlichen Lebensbereich" des Kindes betreffen, ausgenommen der in § 173 ABGB taxativ aufgezählten Situationen.[21] Als Beispiel sei hier die medienrechtliche, durch den OGH bestätigte OLG Wien Entscheidung[22] hinsichtlich des Verbreitens von Lichtbildern einer geistig beeinträchtigten und körperlich versehrten Jugendlichen genannt. Fraglich bleibt, inwieweit der Begriff „höchstpersönlicher Bereich" im Datenschutzrecht ausgestaltet sein wird und ob alle besonderen Daten darunter subsumiert werden können.

Ausblick

Mit der DSGVO werden zusätzliche Parameter zum rechtssicheren Umgang mit Unterhaltungselektronik für Kinder hinzugefügt, die Einzelfallentscheidungen nach sich ziehen werden. Eine wichtige Rolle spielt hierbei die Einwilligung durch die Eltern zur Übermittlung und die Frage, inwieweit diese bei „sensiblen" Daten, die den höchstpersönlichen Bereich betreffen, die Einwilligung des Kindes substituieren kann. Dabei könnte auf eine altersgerechte Abstufung der Eingriffsintensität sowie die Einsichts- und Urteilsfähigkeit des Kindes abgestellt werden.

Dako 2018/5

[15] *Mascheroni/Holloway*, The Internet of Toys: A Report on Media and Social Discourses around Young Children and IoToys 5 ff. [16] http://myfriendcayla.fr/. [17] Antwort der Bundesregierung auf die Kleine Anfrage 18/8317, 3. 5. 2016, 1 f. [18] Siehe Art 6 Abs 1 DSGVO. [19] Zu den Datenkategorien siehe Art 9 DSGVO. [20] Siehe § 173 ABGB. [21] *Haidinger*, Minderjährige in der datenschutzrechtlichen Judikatur, Dako 1/2017, 17 f. [22] OGH Beschluss vom 13. 1. 2016, 15 Os 176/15 v.

Zum Thema

Über die Autorinnen

Mag. Karin Tien ist Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte, Wien. E-Mail: tk@kt.at

Mag. Jennifer Maria Held ist Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte, Wien. E-Mail: jh@kt.at, Internet: www.kt.at

Tobias Tretzmüller
Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte OG

Der globale Anwendungsbereich der DSGVO – warum die DSGVO auch in Drittländern umgesetzt werden sollte (muss)

Räumlicher Anwendungsbereich; Geldbußen; Schadenersatz; Vertrauen; Marktorientierungsprinzip. Die DSGVO gilt für Datenverarbeiter, die ihre Waren oder Dienstleistungen in der EU oder im EWR anbieten. Der territoriale Zuständigkeitsbereich der europäischen Aufsichtsbehörden ist aber auf das eigene Hoheitsgebiet beschränkt. Warum sollten Unternehmen in Drittländern[1] daher die DSGVO umsetzen? Der Beitrag zeigt die Motivationsfaktoren auf.

Räumlicher Anwendungsbereich der DSGVO

Eines der Hauptziele der DSGVO ist die Umsetzung des **Marktorientierungsprinzips:** Unternehmen, die ihre Dienstleistungen oder Waren in der EU anbieten, sollen sich auch den Regeln der DSGVO unterwerfen. Hätte man den räumlichen Anwendungsbereich bloß auf Unternehmen mit Niederlassung in der EU beschränkt, wäre dies – wirtschaftlich betrachtet – einer europäischen Selbstgeiselung gleichgekommen. Ausländische Datenverarbeiter hätten von ihren – hinsichtlich Datenschutz – liberaleren Rechtssystemen profitiert. Am Ende hätten sie ihre zum Teil schon bestehende Marktdominanz ausbauen können. Abgesehen von diesem volksökonomischen As-

[1] Der Begriff Drittland umfasst alle Staaten außer die Mitgliedstaaten der EU sowie die Mitgliedstaaten des EWR (Island, Liechtenstein und Norwegen).

MANZ