MMR

Zeitschrift für IT-Recht und Recht der Digitalisierung

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

CHRISTIAN-HENNER HENTSCH / KONSTANTIN EWALD / ROLF SCHWARTMANN (Hrsg.)

Datenschutz in der Games-Branche. Datenschutzrechtliche Voraussetzungen für ein interaktives Spielerlebnis

Editorial 1 TOBIAS HAAR
Kreatives Jura für eine kreative Branche

Datennutzung 3 JÜRGEN BÄNSCH / CHRISTIAN-HENNER HENTSCH
Datenverarbeitungen in der Games-Branche

Benutzer- und Gerätedaten 8 PATRICK MITSCHING / CHRISTIAN RAUDA
Zeitenwende beim Tracking des Nutzungsverhaltens durch Spiele-Apps

Newsletter-Marketing 12 KAI BODENSIEK / DAVID JULIAN HOFFMANN
Newsletter im Konzern – kein Selbstläufer!

Internationale Datenübermittlung 17 ANDREAS LOBER / SUSANNE KLEIN
Datenschutz bei Multiplayer-Games und Spielen auf sozialen Netzwerken

Machine Learning 22 AXEL VON WALTER
Nutzerdaten, KI und automatisierte Entscheidungsfindung in Games

Sanktionen 27 FLEMMING MOOS
Durchsetzung der DS-GVO mittels Bußgeldern am Beispiel der Games-Branche

Osborne Clarke

Kölner Forschungsstelle für Medienrecht
Technology Arts Sciences TH Köln

game Verband der deutschen Games-Branche

MMR-Beilage
8/2021

Seiten 1–32
24. Jahrgang · 16. August 2021
Verlag C.H.BECK München

1830202108

Schnittstelle: IT · Medien TK · Digitalisierung.

Legal Tech, Smart Contracts, Games, Cybersecurity, Datenschutz u.v.m.

Die MMR ist interdisziplinär wie keine andere Zeitschrift im Recht der neuen und innovativen Medien. Hier finden Sie Informationen zu einschlägigen Themen, die unabdingbar miteinander im Kontext der Digitalisierung verbunden sind. Die MMR bildet die perfekte Schnittstelle zwischen »Recht – IT – KI – Digitalisierung – Medien – TK«. Profitieren Sie vom gesamten Spektrum digitaler Themen, darunter:

- IT- und Softwarerecht
- Big-Data- und Cloud-Anwendungen
- Online-Plattformen und -Handel
- Innovative Beratungs- und Geschäftsmodelle
- Digitalisierung von Behörden und Justiz
- Blockchain, Algorithmen, KI und Robotik
- Plattform-Ökonomie und Intermediäre.

3 Hefte gratis

Kostenloses Schnupperabo:

beck-shop.de/1584

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 141405

C.H.BECK

MMR MultiMedia und Recht

Zeitschrift für IT-Recht und Recht der Digitalisierung

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); Katharina Klauser, Redakteurin; Ruth Schrödl, Redakteurin; Eva Wanderer, Redaktionsassistentin; Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de

twitter.com/MMRZeitschrift
de.linkedin.com/showcase/zeitschriftmmr

Manuskripte: Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag C.H.BECK an seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet.

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Redaktion erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form vervielfältigt, verbreitet oder öffentlich wiedergegeben oder zugänglich gemacht, in Datenbanken aufgenommen, auf elektronischen Datenträgern gespeichert oder in sonstiger Weise elektronisch vervielfältigt, verbreitet oder verwertet werden.

Anzeigenabteilung: Verlag C.H.BECK, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media-Beratung: Telefon 089/3 81 89-687, Telefax 089/3 81 89-589.
Disposition, Herstellung Anzeigen, technische Daten: Telefon (0 89) 3 81 89-609, Telefax 089/3 81 89-589, E-Mail anzeigen@beck.de.
Verantwortlich für den Anzeigenteil: Bertram Mehling

Verlag: Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Der Verlag ist oHG. Gesellschafter sind Dr. Hans Dieter Beck und Dr. h.c. Wolfgang Beck, beide Verleger in München.

Erscheinungsweise: Monatlich.

Bezugspreise 2021: Jährlich € 449,– (inkl. MwSt.). Vorzugspreis für Mitglieder der davit € 355,– (inkl. MwSt.). Alle Abopreise inklusive Newsdienst MMR-Aktuell und MMRDIREKT. Einzelheft: € 45,– (inkl. MwSt.); Versandkosten jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Abonnement und Bezugspreis beinhalten die Printausgabe sowie eine Lizenz für die Online-Ausgabe. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Bestellungen über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag AG (CH) & Co.KG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, E-Mail: zeitschriften@helbing.ch.

KundenServiceCenter: Tel.: 089/3 81 89-750, Fax: 089/3 81 89-358, E-Mail: kundenservice@beck.de

Abbestellungen müssen 6 Wochen vor Jahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an. Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

Satz: FotoSatz Pfeifer GmbH, 82152 Krailling.

Druck: Druckerei C.H.BECK, Bergerstraße 3–5, 86720 Nördlingen.
ISSN 2698-7988

MMR

Zeitschrift für IT-Recht und Recht der Digitalisierung

TK · IT-Security · Medien · Robotik · KI · Datenschutz · Games

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

8/2021 Beilage

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon/Vorstand Deutscher Anwaltverein – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – RA **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., in Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Thomas Hoeren**, Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Bernd Holznagel**, Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Dr. Christine Kahlen**, Leiterin der Unterabteilung VIB, Nationale und europäische Digitale Agenda, Bundesministerium für Wirtschaft und Energie, Berlin – **Dr. Dennis-Kenji Kipker**, Wissenschaftlicher Geschäftsführer am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen, und Mitglied des Vorstands der EAID, Berlin – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – **Dr. Reto Mantz**, Richter am LG, Frankfurt/M. – **Prof. Dr. Alexander Roßnagel**, Universität Kassel/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Köln – **Prof. Dr. Louisa Specht-Riemenschneider**, Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht, Rheinische Friederich-Wilhelms-Universität Bonn – RA **Dr. Axel Spies**, Morgan, Lewis & Bockius LLP, Washington DC – **Prof. Dr. Gerald Spindler**, Universität Göttingen

BEIRAT DER KOOPERATIONSPARTNER

Alisha Andert, Vorstandsvorsitzende des Legal Tech Verband Deutschland e.V., Berlin – **Daniela Beaujean**, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – RAin **Susanne Dehmel**, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – **Dr. Andrea Huber**, LL.M. (USA), Geschäftsführerin, ANGA Verband Deutscher Kabelnetzbetreiber e.V., Berlin

REDAKTION

Anke Zimmer-Helfrich, Chefredakteurin –
Katharina Klauser, Redakteurin –
Ruth Schrödl, Redakteurin –
Eva Wanderer, Redaktionsassistentin –
Wilhelmstr. 9, 80801 München

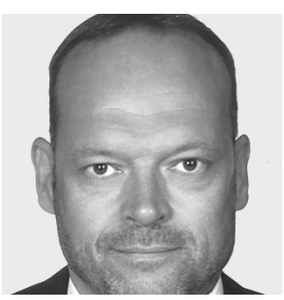
EDITORIAL

Kreatives Jura für eine kreative Branche

Lesedauer: 9 Minuten

Wenn Kreativität auf Recht und Regulierung trifft, eröffnen sich für Jurist*innen unendliche Weiten. Das trifft auf die Computerspielbranche im besonderen Maße zu. Seit über 20 Jahren befassen sich Jurist*innen in aller Welt mit den besonderen Rechtsfragen dieser Branche. Dabei kommen sie mit allen möglichen Rechtsgebieten in Berührung, auch solchen, die in diesem Kontext zunächst gar nicht als besonders relevant erscheinen: Die Herausforderungen reichen dabei von Fragen der Zulässigkeit staatlicher Beihilfe über umsatz- und quellensteuerliche Aspekte, dem Ausländerrecht, aber auch der Exportkontrolle oder der Zulässigkeit polizeilicher Auskunftsanfragen.

Hinzutreten die „klassischen Games-Rechtsthemen", wie Urheberrecht, Patentrecht, Datenschutzrecht, Jugendschutzrecht, Verbraucherschutzrecht, Kartellrecht usw. Einen besonderen Schwerpunkt bildet zudem die Durchsetzung der Rechte der Marktteilnehmer und dabei in erster Linie der Entwickler*innen und Publisher*innen von Games. Da sich diese sowohl im In- wie Ausland befinden oder tätig sind, stellen sich neben nationalen und EU-rechtlichen Rechtsfragen auch solche anderer Rechts- und Kulturkreise. Ein Beispiel mag die zunächst exotisch anmutende Frage sein, inwieweit bestimmte Begrifflichkeiten und Bezeichnungen von Gegenständen in Computerspielen in anderen Ländern aus kulturellen, religiösen oder rechtlichen Gründen unzulässig sind. Besonderen Einfluss haben solche Aspekte gerade auch auf das internationale Jugendschutzrecht.



Tobias Haar

Neben dem geschriebenen „staatlichen" Recht, nimmt der Bereich des durch z.B. App-Plattformen oder Spiele-Plattformen gesetzten „Soft Law" an Relevanz zu. Als Beispiel seien hier etwa die von *Apple* jüngst eingeführte Funktion der App-Tracking-Transparenz oder die Google Safety Section genannt. Meist mangelt es den Spieleanbietern an einer entsprechenden Verhandlungsposition gegenüber diesen übermächtigen Plattformanbietern. Oftmals helfen hier die Erwägungen des nationalen Rechts der Allgemeinen Geschäftsbedingungen wenig, wenn die entsprechenden Verträge etwa US-amerikanischem Recht unterliegen. Gleichzeitig bleiben „nationale" Rechtsakte, wie die DS-GVO weiterhin anwendbar und gehen dieser Form „privater Rechtsetzung" grundsätzlich vor. Es stellen sich mithin Fragen auf mehreren Ebenen miteinander konkurrierender Regularien. Konflikte sind vorprogrammiert und Lösungen mitunter schwierig.

Es ist auch weiterhin zu bedauern, dass Fragen und Grundzüge der Vertragsgestaltung und -verhandlung in der juristischen Ausbildung hierzulande eine allzu untergeordnete Rolle spielen. Alle „Games Lawyers" müssen hier über entsprechende Erfahrung

verfügen. Komplexe Co-Publishing-Verträge, Verträge mit Influencer*innen, eSports-Anbietern und eSportler*innen gehören ebenso zu den wiederkehrenden Themen, wie gesellschaftsvertragsrechtliche Fragen etwa im Bereich der Gründung oder Beteiligung an Entwicklungsstudios im In- wie Ausland. Steuerrechtlichen Fragen kommt gerade in diesen Bereichen eine zentrale Bedeutung zu. Hier werden Kompetenzen verlangt, die allzu oft erst nach erfolgreichem Bestehen der Zweiten Juristischen Staatsprüfung von der Pike auf erlernt und vermittelt werden müssen.

Die o.g. juristischen Herausforderungen verlangen den in der Gamesbranche tätigen Inhouse-Jurist*innen oder beratenden Rechtsanwält*innen schließlich ein besonderes Verständnis der technischen und sonstigen Abläufe von Computerspielen sowie der wirtschaftlichen Interessen der Marktteilnehmer ab – und dies nicht nur für die Beantwortung kartellrechtlicher Fragestellungen. Gerade bei der Vertragsgestaltung ist oftmals „kreatives Jura" gefragt, wenn z.B. neue Formen der angemessenen Teilung von Vermarktungserlösen zwischen Spieleentwickler und Publisher herausgebildet und in Vertragssprache übersetzt werden müssen.

Einen wichtigen Beitrag für die sowohl (rechts-)wissenschaftliche Betrachtung als auch für die Diskussion praktischer Lösungsansätze erbringt hier die MMR nun im vierten Jahr mit ihrer alljährlichen Beilage zu Recht und Games. Folgende wichtige Themen der Gamesbranche wurden beleuchtet: 2018 Recht des eSport, 2019 Rechtsdurchsetzung, 2020 Jugendschutzrecht. Wie aufgezeigt, gibt es Stoff für viele Weitere.

Dem Thema dieser Beilage, dem Datenschutzrecht, kommt eine besondere Stellung bei Computerspielen zu. Heutzutage sind sie entweder meist als Client- oder Browserspiele mit Online-Funktionen versehen oder werden als Smartphone-App heruntergeladen und gespielt. Die Zahl der rein offline spielbaren Computerspiele nimmt laufend ab – aber es gibt sie auch weiterhin. Das Datenschutzrecht kommt bereits ins Spiel, wenn ein Spiel zum ersten Mal heruntergeladen wird. Dieses muss gar nicht über In-Game-Online-Funktionen verfügen, um datenschutzrechtliche Fragen auszulösen. Sie begleiten den Spieleanbieter dann über den Gebrauch des Spiels durch den Nutzer hinaus.

Unbestritten hat die DS-GVO ein Schlaglicht auf das Datenschutzrecht geworfen. Einerseits hat sich am Grundsatz des Verbots mit Erlaubnisvorbehalt nichts geändert, andererseits hat dieses Rechtsgebiet einen starken Wandel hin zur stärkeren Eigenverantwortung der verantwortlichen Stellen erfahren – mit Vor- und Nachteilen. Der signifikant erhöhte Bußgeld- und Sanktionskatalog tun sein Übriges, um die gewünschte Aufmerksamkeitssteigerung zu erreichen.

Die DS-GVO ist vor gut drei Jahren mit großem Knall an den Start gegangen. Unzählige Stunden von Juristenarbeit sind in Compliance-Programme und die Aufklärung sowie Schulung anderer Fachbereiche geflossen. Inzwischen macht sich jedoch Ernüchterung breit und Aussagen wie „Eine 100-prozentige Datenschutz-Compliance ist gar nicht möglich und nun einmal zu akzeptieren" sind nicht selten. Regulierung in Form einer DS-GVO muss mit unbestimmten Rechtsbegriffen arbeiten. Jurist*innen sind es gewohnt, mit den damit verbundenen Herausforderungen umzugehen.

Wenn dann aber noch hinzukommt, dass die Datenschutzaufsicht in mehreren Ländern teils unterschiedliche Herangehensweisen und ein durch unterschiedliche Finanzierungskonzepte sowie politische Einflussnahme geprägtes mitunter größeres oder geringeres Interesse an der Rechtsdurchsetzung hat und eher mit oder eher gegen die Anbieter von Computerspielen (und selbstverständlich anderen Bereichen) agiert, steht eine internationale Branche vor großen Problemen. Die Computerspieleindustrie leidet sehr unter der uneinheitlichen Anwendung und Auslegung datenschutzrechtlicher Vorgaben, nicht nur unter der DS-GVO innerhalb der EU, sondern darüber hinaus. Im Datenschutzrecht wird das Warten auf Klarstellungen durch den *EuGH* leider zum Dauerzustand. Und hat er dann endlich entschieden, wie im Schrems-II-Urteil, hören die Unsicherheiten nicht auf, sondern beginnen mitunter erst. Der Brexit war in diesem Zusammenhang ebenfalls nicht hilfreich.

Der Bedeutung des Datenschutzes und die juristische Diskussion für die Gamesbranche wird die MMR mit dieser Beilage und den ausgewählten Themen gerecht. Seit Jahren verbindet die Autor*innen eine offene Austausch- und Diskussionskultur in Form von Arbeitsgemeinschaften oder Juristentreffen auf der gamescom und dergleichen. Mit großem Einsatz und viel Energie werden deren Treffen vorbereitet und durchgeführt – in Pandemiezeiten profitiert die Branche in den unerlässlich gewordenen virtuellen Veranstaltungen von den zuvor geknüpften teils engen Freundschaften und schafft es dennoch, neue Mitglieder für ihre Arbeitsgemeinschaften anzusprechen und zu integrieren.

Diese Arbeitsgemeinschaften, insbesondere des *game – Verband der deutschen Games-Branche e.V.*, waren und sind unerlässlich, um ein möglichst einheitliches Verständnis für Rechtsfragen zu gewinnen. Sie ermöglichen es den Unternehmensjurist*innen zudem, bei knappen Ressourcen in Rechtsabteilungen auf ein großes Wissen in – wie beschrieben – auch exotischen Rechtsgebieten zurückgreifen zu können. Sie ermöglichen es auch, in den Austausch mit Politik sowie anderen Branchen und deren Interessengemeinschaften zu treten. Und das Ganze nicht nur auf nationaler, sondern auch internationaler Ebene, wie erfolgreiche Veranstaltungsformate (z.B. der Games Industry Law Summit in Vilnius) eindrucksvoll belegen. Der *game* hat mit seinem vor gut drei Jahren erfolgten Zusammenschluss aus G.A.M.E. und BIU in diesem Bereich an Bedeutung gewonnen. Wer hätte es gedacht, wie erfolgreich sich diese Arbeitskreise entwickelt würden, als sich einige Inhouse-Jurist*innen vor über zehn Jahren zum Erfahrungsaustausch über die richtige Umsatzbesteuerung von später sog. „elektronisch erbrachten Leistungen" verabredeten und gemeinsam mit dem *Bundesministerium der Finanzen* in Kontakt traten?

Meine Aufgabe als Sprecher der *Arbeitsgemeinschaft Recht* nehme ich mit großer Freude wahr. Mit zahlreichen Teilnehmer*innen verbinden mich Freundschaften und die Lust an Diskussion und Horizonterweiterung in den vielen Rechtsthemen der Branche. Wir können dabei aus einem großen Fundus an Berufs- und Lebenserfahrungen schöpfen. Unser Diskurs stützt sich breit auf Inhouse-Jurist*innen wie Rechtsanwält*innen, auf Institutionen wie die *Unterhaltungssoftware Selbstkontrolle (USK)* sowie dem *game* und seinen Mitgliedern insgesamt. Ein besonderes Lob verdienen hier die Geschäftsstelle des Verbands und ihr Leiter Recht & Regulierung, der Mitherausgeber der MMR und Initiator der Beilagen *Christian-Henner Hentsch*. Als *AG Recht* des *game* werden wir auch weiterhin Workshops zu Datenschutz und vielen anderen Rechtsthemen abhalten. Zuletzt haben wir uns z.B. mit Webinaren um Rechtsfragen des Brexit oder der Rechtsdurchsetzung beschäftigt. Und im kommenden Jahr werden wir als „Games Lawyer" gerne wieder an einer weiteren Schwerpunktausgabe der MMR mitwirken.

Wir laden alle interessierten Kreise ein, mit uns gemeinsam diesen fruchtbaren Diskurs und Austausch fortzusetzen und weiter zu intensivieren. An Themen für künftige Schwerpunktausgaben der MMR mangelt es nicht, wie auch das alsbald erscheinende „Handbuch Games und Recht" eindrücklich beweisen wird. Es bleibt also spannend im „Gamesrecht" – sehr spannend.

Berlin, im August 2021

Tobias Haar
ist Sprecher der Arbeitsgemeinschaft Recht des game – Verband der deutschen Games-Branche e.V. und Rechtsanwalt in Karlsruhe.

JÜRGEN BÄNSCH / CHRISTIAN-HENNER HENTSCH

Datenverarbeitungen in der Games-Branche

Das Spielerlebnis zwischen Vertragserfüllung, berechtigtem Interesse und Einwilligung

Datennutzung

In Computerspielen werden aus vielen unterschiedlichen Gründen Daten erhoben und verarbeitet, sei es für den Spielvorgang und die Kommunikation im Multiplayer-Modus, für die Bezahlung und Bereitstellung von Zusatzinhalten, zur Verbesserung des Spielerlebnisses und zur Entwicklung neuer Spiele oder auch für Werbung. Die meisten dieser Datenverarbeitungen erfolgen zur Erfüllung eines Vertrags bzw. einer rechtlichen Verpflichtung oder zur Wahrung berechtigter Interessen, nur selten sind Einwilligungen erforderlich. I.E. ist die DS-GVO nach drei Jahren in der Games-Branche fest implementiert und es haben sich „Best Practices" herausgebildet. Die einheitlichen Regelungen haben sich grundsätzlich bewährt, auch wenn die Regelungen zu Tracking und zum Datentransfer in Drittstaaten sowie eine sehr unterschiedliche Auslegung der DS-GVO durch die europäischen Aufsichtsbehörden weiterhin Probleme bereiten. Lesedauer: 22 Minuten

I. Einführung: Bedeutung von Daten für die Games-Branche

Daten sind das Lebenselixier für Computer- und Videospiele. Die Games-Branche ist auf die Daten ihrer Nutzer*innen angewiesen, um ein interaktives Spielerlebnis zu ermöglichen und vor allem auch immer wieder zu verbessern und entsprechend der Spielgewohnheiten der Nutzer*innen optimieren zu können. So wichtig wie die Daten für die Games-Branche sind, ist entsprechend auch das Datenschutzrecht zu einer zentralen Rechtsmaterie für die Branche geworden. Allerdings gibt es im Datenschutz für Games keine speziellen Regelungen, sodass die allgemeinen Vorschriften der DS-GVO und des BDSG bei personenbezogenen Daten zur Anwendung kommen, i.Ü. greifen die Bestimmungen des TMG. Diese Regelungen sind abstrakt-generell und natürlich nicht auf die Games-Branche abgestimmt. Bei deren Anwendung kommt es maßgeblich auf das jeweilige Geschäftsmodell an, welche Daten überhaupt benötigt werden und dazu erhoben und verarbeitet werden. Da jedoch die meisten Spiele inzwischen eine Online-Anbindung haben, einen Spieler-Account verlangen und meist auch einen Multiplayer-Modus anbieten, werden bei nahezu allen Spielen personenbezogene Daten erhoben. Dabei werden Daten insbesondere für die Bereitstellung des Spiels, für Abrechnungszwecke und zur Verbesserung des Spielerlebnisses verarbeitet. Die Datennutzung für Werbung bzw. zur Refinanzierung durch Werbung, wie bei vielen anderen Mediengattungen, findet in ganz vielen Spielen nicht statt. Insofern unterscheidet sich die Games-Branche doch erheblich von den anderen Medien und hat stattdessen ganz andere Interessen und damit auch rechtliche Herausforderungen. Um diese Besonderheiten herauszuarbeiten, wird in diesem Beitrag zunächst dargestellt, welche Arten von Daten typischerweise in einem Computer- und Videospiel gesammelt, verarbeitet und gespeichert werden (II.). Es wird dabei auch erklärt, welche Daten so essenziell sind, dass ein Game ohne sie nicht funktionieren würde. Dadurch soll aufgezeigt werden, welche zentrale Rolle Daten in der Wertschöpfungskette von Games spielen. Im Anschluss wird erläutert, welche typischen Gründe für eine rechtmäßige Datenverarbeitung nach Art. 6 DS-GVO meist vorliegen (III.). Neben der Vertragserfüllung und dem berechtigten Interesse wird auch auf das Consent Management und die Einwilligung bei Minderjährigen eingegangen. Nachfolgend werden besondere Aspekte bei Tracking, Auftragsdatenverarbeitungen bzw. gemeinsamen Datenverarbeitungen und beim Datentransfer in Drittstaaten thematisiert (IV.).

II. Datenverarbeitungen in der Games-Branche

Als Geschäftsmodell besteht das Wesen eines Computer- oder Videospiels darin, ein spannendes und interessantes Spielerlebnis zu bieten. Es handelt sich also um eine digitale und interaktive Dienstleistung, für die Daten essenziell sind. Damit diese Dienstleistung bereitgestellt werden kann, bedarf es daher mehrerer Kategorien von Daten. Typischerweise, aber nicht abschließend, werden rein funktional-technische Daten erhoben und verarbeitet wie Account-Daten, Gameplay-Daten, Kommunikations- und Interaktionsdaten sowie Daten von Dritten.[1]

1. Geräte- und Netzwerkdaten

Für jedes Computerspiel – egal ob auf PC, Konsole oder Mobile Device – muss in der Regel eine Verbindung zwischen den Servern des Anbieters und dem Spielergerät hergestellt werden. Dies erfordert die Erfassung und Verarbeitung von technischen Informationen in Bezug auf die Konfigurationen des Netzwerks, des Geräts und der angeschlossenen Peripheriegeräte wie Controller und Headsets. Beispiele für solche Geräte- und Netzwerkdaten sind MAC- und IP-Adressen, Seriennummern der Geräte, Daten des Internetdiensteanbieters oder des Mobilfunkanbieters. Diese Art von Daten kann auch Informationen über die Software oder Anwendungen umfassen, die auf dem Gerät installiert sind und wie sie vom Player verwendet werden. Obwohl diese Daten technischer Natur sind, sollten sie meist als personenbezogene Daten betrachtet werden, da es damit möglich ist, die Identität des Spielers direkt oder indirekt zu offenbaren. Im letzteren Fall sollte die Fähigkeit eines Dritten, die Daten rechtmäßig mit ergänzenden identifizierbaren Informationen zu kombinieren, immer vorausgesetzt werden, wenn eine solche Aktivität ein „Mittel darstellen würde, das vernünftigerweise verwendet werden könnte".[2] Die Erhebung und Verarbeitung dieser Art von Daten erfordert häufig einen direkten Zugriff auf Informationen und Verarbeitungs- und Speichermöglichkeiten

1 Vgl. hierzu z.B. die Nintendo Privacy Policy, die Kategorien von Daten aufführt, abrufbar unter: https://accounts.nintendo.com/term/privacy_policy/US?lang=en-US sowie sehr detailliert die Datenschutzerklärung von EA, abrufbar unter: https://tos.ea.com/legalapp/WEBPRIVACY/DE/de/PC/#section1.

2 Vgl. zu dynamischen IP-Adressen *EuGH* MMR 2016, 842 m. Anm. *Moos/Rothkegel* – Breyer.

des Geräts des Spielers durch die Verwendung von Cookies oder ähnlichen Technologien und unterliegt dann anderen rechtlichen Anforderungen nach dem Datenschutzrecht für elektronische Kommunikation.

2. Account-Daten

Die Teilnahme an einem Online-Spiel setzt regelmäßig eine Registrierung mit einem Account voraus, wobei der Spieler zumindest grundlegende Kontaktinformationen und Profilinformationen angeben und einen Benutzernamen und ein Passwort seiner Wahl festlegen muss. Zunächst werden als personenbezogene Daten bei der Anmeldung bzw. Registrierung Namen und E-Mail-Adressen erhoben und aus Jugendschutz- und Datenschutzgründen oft auch das Alter.[3] Teilweise reichen für die kostenfreie Nutzung von Online-Spielen auch die Angabe einer E-Mail-Adresse, ggf. eines Benutzernamens und eines Passworts. Passwörter werden üblicherweise in haschierter Form gespeichert, die zu keiner Zeit einen Rückschluss auf das tatsächliche Passwort erlaubt. Bei der Inanspruchnahme von kostenpflichtigen Diensten sind neben dem Namen auch die Anschrift und Kontodaten erforderlich. Für die Bearbeitung von Anfragen oder zur Kundenbetreuung können neben dem Namen, der Adresse und der E-Mail-Adresse auch Telefonnummern verarbeitet werden. Um den Kauf von Inhalten zu ermöglichen, werden auch wesentliche Rechnungsdaten wie die physische Adresse und die Kreditkartennummer benötigt. Kontodaten können sensible Informationen enthalten und sind oft mit anderen personalisierten Informationen über beliebte Spieletitel, Spielstände und Erfolge, Kommunikations- und Marketingpräferenzen usw. verknüpft. Benutzernamen oder Gamer-Tags sind eine gängige Form von pseudonymisierten Daten und ermöglichen es Spieler*innen, miteinander zu interagieren und gleichzeitig ihre Identität zu schützen.

3. Gameplay-Daten

Wenn Spieler*innen mit dem Spiel oder mit anderen Spielen in Multiplayer-Spielen interagieren, werden Daten über ihre Aktivitäten generiert. Diese Daten spielen eine wesentliche Rolle bei der Art und Weise, wie Unternehmen Softwarefehler oder Bugs und betrügerisches Verhalten der Spieler*innen erkennen. Sie werden auch verwendet, um das Spielerlebnis für die Spieler*innen zu verbessern, z.B. um Engpässe innerhalb des Spiels zu finden, an denen viele Spieler*innen an den gestellten Aufgaben scheitern. Durch die kollektive Analyse der Spielerdaten kann ein Games-Unternehmen feststellen, ob es ein größeres Problem gibt, das von der Mehrheit der Spieler*innen erlebt wird und lernen, wie es behoben werden sollte. Entwickler und Publisher stellen daher regelmäßig Updates und Patches für Spiele bereit, die bestehende Inhalte und Benutzererfahrungen ergänzen und verbessern können. Die Analyse von Gameplay-Daten hilft auch dabei, Spieler*innen auf der Basis von nicht präzisem Standort und ihren Fähigkeiten zu erkennen, ohne sie weiter identifizieren zu müssen. Spieler*innen haben ein besseres Spielerlebnis, wenn sie mit anderen Spieler*innen mit ähnlichen Fähigkeiten zusammengeführt werden. Der Standort ist erforderlich, um sicherzustellen, dass die Spieler*innen auf den am besten gelegenen Servern zusammengeführt werden, damit ihre Verbindungen nicht unterbrochen werden. Ähnlich wie Geräte- und Netzwerkdaten können auch Spielverlaufsdaten, oft nur indirekt, die Identität des Spielers offenbaren und können daher in diesen Fällen als personenbezogene Daten betrachtet werden.

4. Kommunikations- und Interaktionsdaten

Zu den Spieldiensten gehören im Allgemeinen auch Kommunikationsfunktionen innerhalb der Spielsoftware, die die Kommunikation zwischen Spieler*innen oder zwischen dem Spieler und dem Anbieter des Spiels ermöglichen. Solche zusätzlichen Kommunikationsdienste unterstützen die Spielaktivitäten, indem sie es den Spieler*innen ermöglichen, eine Spielverabredung im Voraus zu planen und während des Spiels zu kommunizieren. Sie ermöglichen es dem Spieler auch, Fehlfunktionen, unangemessene Inhalte oder missbräuchliches Verhalten zu melden.[4] Die Kommunikation mit dem Anbieter kann auch außerhalb der Spielesoftware stattfinden, wenn sie notwendig ist, um auf Anfragen zu reagieren, Produktsupport zu leisten oder Mitgliedsfunktionen zu aktivieren wie z.B. die Möglichkeit, exklusive Inhalte zu erhalten, Preise für Wettbewerbe einzulösen oder Newsletter geschickt zu bekommen. Der Inhalt einer Kommunikation sowie die zugehörigen Metadaten, die für die Zwecke ihrer Übermittlung verarbeitet werden, können sehr sensible und persönliche Informationen offenbaren und unterliegen daher grundsätzlich den strengen Vertraulichkeitsanforderungen. Kommunikationsdienste in Computerspielen wie z.B. eine Chat-Funktion in einem Online-Spiel sind zwar regelmäßig kein interpersoneller Telekommunikationsdienst nach § 3 Nr. 23 TKG, weil es sich hierbei um eine unbedeutende Nebenfunktion i.V.m. einem anderen Dienst handelt.[5] Allerdings greifen hier die Datenschutzvorschriften des TMG und absehbar auch die neuen Regelungen der noch verhandelten Datenschutzverordnung für elektronische Kommunikation (ePrivacy). Nach der geplanten Überarbeitung der ePrivacy-RL wird es wohl – unabhängig vom Personenbezug – künftig nicht mehr möglich sein, Chat-Funktionen oder andere Begleitdienste aktiv oder reaktiv zu überwachen, die nicht allen Spieler*innen offenstehen, sondern eine Verbindung zwischen einer begrenzten Anzahl von Spieler*innen ermöglichen, wenn diese selbst entscheiden können, mit wem sie sich verbinden.

5. Daten von Drittanbietern

Online-Gameplay-Dienste verarbeiten nicht nur Daten, die sie direkt vom Spieler erhalten oder gesammelt haben. Informationen werden auch von externen Drittanbietern weitergegeben oder mit diesen geteilt. Dabei handelt es sich mehrheitlich um Anbieter, die an der technischen Bereitstellung des Dienstes beteiligt sind, z.B. Spieleplattformen, Datenanalyseunternehmen und Finanzinstitute, die Zahlungstransaktionen verifizieren. Darüber hinaus können Daten auch an Verwaltungs- oder Justizbehörden weitergegeben werden, um einer gesetzlichen Verpflichtung nachzukommen, z.B. im Zusammenhang mit einer Untersuchung von Betrug oder der Verletzung geistigen Eigentums oder zum Schutz der Persönlichkeitsrechte und der Sicherheit der Spieler*innen. In diese Datenkategorie können auch Daten fallen, die zum Zweck der Bereitstellung personalisierter Werbung oder personalisierter Inhalte für den Spieler freigegeben werden. Anbieter wie soziale Netzwerke oder andere Videospiel-Publisher können Informationen über den Spieler weitergeben, wenn er sich entschieden hat, sein Konto mit diesen Diensten zu verknüpfen. Teilweise werden Daten auch direkt mit Marketingunternehmen geteilt. Gezielte Werbung erfordert eine Analyse der persönlichen Daten eines Spielers, um Merkmale oder Verhaltensmuster zu erkennen und Vorhersagen treffen zu können. Der Austausch von Daten zum Zweck der geziel-

3 Aus Gründen der Datensparsamkeit empfiehlt sich lediglich die Abfrage, ob ein gewisses Alter erreicht ist. Bei dauerhaften Nutzungen lässt sich dies allerdings nur mit dem Geburtsdatum feststellen. Auch zur Einhaltung des Jugendschutzes ist meist das exakte Alter abzufragen.

4 Das JuSchG und viele weitere Gesetze setzen solche Meldemöglichkeiten sogar explizit voraus. Auch im DSA werden umfassende Meldemöglichkeiten diskutiert.

5 Mit dem neuen Telekommunikationsmodernisierungsgesetz wurde der am 20.12.2018 in Kraft getretene Europäische Kodex für die elektronische Kommunikation (RL (EU) 2018/1972) umgesetzt. Im Erwägungsgrund 17 werden ausdrücklich Kommunikationskanäle in Online-Spielen als Regelbeispiele genannt, die danach nicht unter diesen Begriff des „interpersonellen Kommunikationsdienstes" fallen; vgl. auch *Kollmann*, MMR 2021, 462.

ten Werbung ist jedoch kein übliches Geschäftsmodell in der Games-Branche und die Bedeutung nimmt sogar eher ab. Die Refinanzierung erfolgt anders als in vielen anderen Medienbranchen vor allem über Verkäufe der Spiele, In-Game-Käufe sowie Abo-Modelle und Gebühren für Services.

III. Rechtmäßigkeitsgründe bei der Datenverarbeitung

Die o.g. üblichen Datenverarbeitungen in Computerspielen müssen natürlich rechtmäßig erfolgen und stützen sich dabei in der Regel auf die Erlaubnistatbestände des Art. 6 DS-GVO. Die dort aufgezählten Rechtsgrundlagen gelten grundsätzlich gleichrangig nebeneinander. Auf Grund der direkten Vertragsbeziehungen zwischen Anbietern von Games und deren Spieler*innen erfolgen die mit Abstand meisten Datenverarbeitungen zur Erfüllung eines Vertrags. Auch berechtigte Interessen rechtfertigen viele Datenverarbeitungen. Eine Einwilligung wird meist nur dann eingeholt, wenn sie wirklich nötig ist.

1. Vertragserfüllung

Mit dem Vertrag über den Kauf und die Nutzung eines Computerspiels verpflichtet sich der Anbieter, das Spiel bereitzustellen und einen technisch reibungslosen Spielverlauf zu gewährleisten.[6] Um diesen Vertragspflichten nachzukommen, müssen jedenfalls die Geräte- und Netzwerkdaten erhoben werden, damit das Game auf dem vom Nutzer gewünschten Gerät gespielt werden kann. Auch die Account-Daten werden i.R.d. Vertragserfüllung vor allem zu Abrechnungszwecken, aber auch zur Einhaltung der Jugendschutzbestimmungen benötigt. Auch die Gameplay-Daten werden vor allem für die Ermöglichung des Spielerlebnisses genutzt. Denn ohne den Multiplayer-Modus oder die Ortungsfunktion bei einem Location-based Game wie Pokémon Go sind wesentliche Spielfunktionen rein technisch gar nicht möglich. Auch das Erkennen von Bugs, Betrug, Bots oder Trollen trägt zum Funktionieren eines Spiels bei und ist somit von der Vertragserfüllung gedeckt. Bei Kommunikations- und Interaktionsdaten ist zu unterscheiden zwischen der Bereitstellung von Kommunikationsmitteln für Spielverabredungen und die Abstimmung im Spiel und der Kommunikation zwischen Anbieter und Nutzer. In beiden Fällen kann es nach der DS-GVO um die Erfüllung des Vertrags gehen, wenn etwa die Kommunikation zum Spielerlebnis gehört oder Meldefunktionen einen reibungslosen Ablauf sichern sollen.[7] Bei Marketing-Maßnahmen, die keinen Bezug zum Spielverlauf haben, oder bei Maßnahmen gegen Toxic-Player wird die Verarbeitung auf andere Rechtmäßigkeitsgründe gestützt sein. Auch die Weitergabe von personenbezogenen Daten an Dritte kann der Vertragserfüllung dienen, soweit diese an der technischen Bereitstellung des Spiels oder der Abrechnung beteiligt sind. All diese Verarbeitungen werden meist nicht nur in der Datenschutzerklärung, sondern auch in den EULA (End User License Agreement) bzw. dem Account User Agreement aufgeführt.[8]

2. Berechtigtes Interesse

Neben der Vertragserfüllung spielt bei der rechtmäßigen Verarbeitung von personenbezogenen Daten der Spieler*innen eines Games auch das berechtigte Interesse eine wichtige Rolle. So bieten viele Publisher ihren Spieler*innen individuell zugeschnittene Zusatzinhalte und Spielerlebnisse an. Dabei handelt es sich um besondere Skins oder Ausrüstungsgegenstände, um neue Level und Erweiterungen sowie vergleichbare Spiele des gleichen Herstellers. Diese Leistungen sind gerade nicht Vertragsbestandteil, sondern neue In-Game-Käufe, die über ein gesondertes Rechtsgeschäft erworben werden. Trotzdem werden viele dieser Angebote meist doch gewünscht und oft auch gerne angenommen. Entsprechend werden hier Daten für die Bereitstellung von zielgerichtetem Marketing verarbeitet, vor allem durch den eigenen Kundendienst, manchmal auch durch einen Dienstleister. Grundsätzlich kann auch Direktwerbung ein berechtigtes Interesse darstellen, wie in Erwägungsgrund 47 DS-GVO norminterpretierend festgeschrieben ist. Dabei ist natürlich eine Interessenabwägung zwischen dem berechtigten Interesse „Marketing" – unter Berücksichtigung der Umstände des konkreten Einzelfalls – mit den entgegenstehenden Interessen und Rechtspositionen der betroffenen Personen vorzunehmen. Insbesondere ist hier darauf abzustellen, was objektiv durch betroffene Personen vernünftigerweise erwartet werden kann. Es ist also darauf abzustellen, ob die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung in bestimmten Bereichen der Sozialsphäre als sozialtypisch akzeptiert oder vielmehr abgelehnt wird. In der Games-Branche sind In-Game-Käufe absolut üblich und für die meisten Free-to-Play-Spiele (F2P) sogar die einzige Einnahmequelle. Insoweit muss davon ausgegangen werden, dass jedenfalls Angebote für Virtual Items und Erweiterungen sozialtypisch akzeptiert und daher auch gerechtfertigt sind. Zum Schutz von Kindern gibt es für Werbung und Profiling besondere Vorgaben (Erwägungsgrund 38 DS-GVO). Daneben sind auch die Vorgaben von § 7 UWG einzuhalten, die allerdings bei Direktwerbung gegenüber Bestandskunden wie in diesem Fall zu keinem anderen Ergebnis führen.

3. Einwilligungen

Eine Einwilligung ist in allen anderen Fällen erforderlich, in denen die o.g. Ausnahmen nicht greifen. In der Praxis stellt sich die Einwilligung also als Auffang-Rechtfertigung dar. Vor allem im Bereich personalisierter Werbung oder bei personalisierten Inhalten sowie bei Spielen über soziale Netzwerke oder bei Verknüpfungen des Accounts mit diesen Diensten muss in der Regel eine Einwilligung eingeholt werden. Dies gilt auch bei besonderen Kategorien von Daten nach Art. 9 DS-GVO, die allerdings in Spielen nur sehr selten erhoben werden. Allerdings sind künftig auch Spiele denkbar, die z.B. über die VR-Brille Gesundheitsdaten registrieren können. Auch beim Tracking und Profiling sind Einwilligungen zwar im Grundsatz gesetzlich, können aber gem. Art. 22 Abs. 2 DS-GVO gerechtfertigt sein. Bei Online-Games wird die Einwilligung meist auf der Landingpage über eine firmeneigene Plattform für Einwilligungs-Management eingeholt. Bei PC- und Konsolen-Spielen erfolgt die Einwilligung bei der Registrierung bzw. dem ersten Starten des Spiels. Durch das neue App Tracking Transparency Framework (ATT) bei *Apple* wird die Einwilligung für Tracking nun zentral und einmalig von der Plattform abgefragt.[9] Um frühe Abbrüche zu vermeiden und die sog. Conversion-Rate[10] zu erhöhen, könnte die Einwilligung erst nach einem Tutorial abgefragt werden. In § 327q Abs. 2 BGB ist nun klargestellt worden, dass Spieler*innen bei einem Widerspruch gegen die Verwendung seiner/ihrer Daten bzw. einem Widerruf das weitere Spielen verweigert werden kann.[11] Einwilligungen können natürlich weiterhin gem. Art. 7 Abs. 3 DS-GVO jederzeit widerrufen werden. Im Falle einer Vertragsbeendigung ist ein Widerruf der Einwilligung nicht erforderlich,

6 Mit dem Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen werden die vertraglichen Hauptleistungspflichten und die Vertragsmäßigkeit in den §§ 327b ff. BGB explizit aufgeführt und z.B. auch neue Update-Pflichten begründet, § 327f BGB.

7 Nach der künftigen ePrivacy-VO muss dafür wohl stets eine Einwilligung vorliegen, wenn es sich um eine Verbindung zwischen einer begrenzten Anzahl von Spieler*innen handelt, die selbst entscheiden können, mit wem sie sich verbinden.

8 So z.B. bei der Spieleplattform EA Origin, abrufbar unter: http://tos.ea.com/legalapp/eula/DE/de/ORIGIN/.

9 Hintergründe und Auswirkungen dieses neuen Frameworks beleuchten in dieser Beilage ausführlich *Mitsching/Rauda*.

10 Die Conversion Rate (CRV) ist das Verhältnis der Besucher*innen einer Webseite zur Anzahl der Abschlüsse, hier also der neu gewonnenen Spieler*innen.

11 Anders wohl in Kalifornien, denn im CCPA gilt ein Diskriminierungsverbot bei der Ausübung von Widerspruchsrechten.

denn über § 327q Abs. 1 BGB wird auf die Bestimmungen der DS-GVO verwiesen.

Eine besondere Herausforderung ist die Einwilligung bei Minderjährigen. Gem. Art. 8 Abs. 1 S. 1 DS-GVO können Minderjährige, die ihr 16. Lebensjahr vollendet haben, wirksam in die Datenverarbeitung durch Games-Anbieter einwilligen, ohne dass es einer Einwilligung des Sorgeberechtigten bedarf. Die Voraussetzung hierbei ist, dass die Einwilligung (wie sonst auch) ausdrücklich und freiwillig abgegeben sowie die betroffene Person über die konkrete Datenverarbeitung und ihre Betroffenenrechte ausreichend informiert wurde. Sofern das Kind jünger ist, ist die Rechtmäßigkeit der Datenverarbeitung von der Einwilligung des Sorgeberechtigten oder dessen Zustimmung in die Einwilligung abhängig. Dabei muss die Zustimmung des Sorgeberechtigten zeitlich vor der Datenerhebung erfolgen, eine nachträgliche Genehmigung reicht nicht. Bei vielen Computerspielen wird schon auf Grund des Jugendschutzes das Alter der Spieler*innen abgefragt und auch teilweise i.R.d. technischen Jugendschutzes (Parental Control) überprüft. Insoweit kann der Pflicht aus Art. 8 Abs. 2 DS-GVO Genüge getan werden, indem sichergestellt wird, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde. Auch im JuSchG muss seit der Novelle von Mai 2021 in § 10b Abs. 3 JuSchG der Datenschutz als Interaktionsrisiko berücksichtigt werden. Dabei wird ausschließlich auf die Weitergabe von Bestands- und Nutzungsdaten ohne Einwilligung an Dritte abgestellt, womit wohl Tracking-Daten für Werbung gemeint sind.

IV. Tracking

Eine Einwilligung sowohl für personenbezogene wie auch für nicht-personenbezogene Daten braucht es meist auch für Tracking. Sog. Cookies werden als Marketing-Tool sowie zur Verfolgung des Nutzerverhaltens bei fast allen Online- und Browser-Games eingesetzt. Hierbei ist zwischen First-Party-Cookies („eigene Cookies") und Cookies von Drittanbietern zu unterscheiden. Eigene Cookies werden auf der Website eines Browser-Games oder über den App-Store vor allem zur Geräteerkennung, zur Weiterleitung zu den gewünschten bzw. gekauften Settings, zur Anzeige der richtigen Sprachversion und zur Verhinderung von Massenregistrierungen genutzt und sind daher unabdingbar für den Betrieb des Spiels. Es handelt sich dabei also meist um sog. funktionale Cookies. Daneben werden aber auch Third-Party-Cookies von autorisierten Drittanbietern eingesetzt, um das Wechseln zwischen den Seiten des Anbieters und zu anderen Seiten nachverfolgen zu können. Hierbei gibt es zum einen notwendige Cookies zur Erkennung von Download-Problemen oder anderen Spielabstürzen[12] sowie zur Betrugsprävention[13] oder zum Schutz vor Spam[14].

Daneben werden aber auch Cookies von Drittanbietern zu Marketing-Zwecken eingesetzt. Diese dienen zunächst der Erkennung von „Conversion Events", also wann es zu besonders vielen oder wenigen Installationen kam, Registrierungen abgebrochen wurden oder Geld ausgegeben wurde. In der Regel werden diese Informationen aggregiert oder zumindest pseudonymisiert. Die Tracking-Daten ermöglichen aber auch das Ausspielen von Werbung durch Werbenetzwerke und andere Werbeunternehmen sowie anonymisiert die Zurechnung von erfolgreichen Marketingmaßnahmen zu einem bestimmten Marketingpartner wie z.B. Influencer*innen oder Let's-Playern oder die Optimierung auf der Grundlage von Conversions-Zahlen, um Retargeting zu vermeiden, statistische Wiederholungen auszuschließen oder unerwünschte Adressaten zu unterdrücken. Neben Cookies können diese Daten bei Browser-Games über Tracking Links oder die Log-in-Lösungen von Facebook connect, Google Sign-In oder Sign-In mit *Apple* erhoben werden. Bei Mobile Games werden die Daten über Partner Module in Adjust oder AppsFlyer bereitgestellt.

Nach dem *EuGH*-Urteil zu Planet 49[15] ist nunmehr klar, dass der Einsatz von Cookies – unabhängig von der Frage, ob personenbezogene Daten verarbeitet werden – grundsätzlich einer aktiven und freiwilligen Einwilligung nach der ePrivacy-RL bedarf. Nur bei einer Nachrichtenübertragung oder wenn (funktionale) Cookies unbedingt für den vom Nutzer angeforderten Dienst erforderlich sind, kann eine Ausnahme greifen (Art. 5 Abs. 3 ePrivacy-RL). Dies wurde nun auch durch das neue TDDSG festgeschrieben, das zusammen mit dem überarbeiteten Telekommunikationsgesetz zum 1.12.2021 in Kraft treten wird. Nach § 25 TTDSG sind Cookies ohne Einwilligung erlaubt, wenn sie unbedingt erforderlich sind, um einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen zu können (funktionale Cookies). Ein Einwilligungsverzicht gem. § 15 Abs. 3 TMG ist jedenfalls nicht mehr möglich.[16]

Die Einwilligung sollte bei Browser-Spielen bei der Registrierung eingeholt werden, bei Mobile Games beim ersten Spielen. Für Browser-Games wird die Einwilligung häufig über eine Cookie Bar oder ein Banner auf allen Landingpages eingeholt, bei Mobile Games ist dies nicht möglich und erfolgt üblicherweise über den AppStore. In beiden Fällen muss nach der jüngsten Rechtsprechung sichergestellt sein, dass das Consent Management nicht übersprungen werden kann, eine Auswahl möglich ist und die Voreinstellung auf Opt-out gesetzt ist. Einige Browser[17] lassen Third-Party-Cookies zu Marketing-Zwecken gar nicht mehr zu. Auch Ad-Blocker können solche Cookies verhindern, nicht jedoch First-Party-Cookies, die aus technischen Gründen nötig sind.

V. Weitergabe von Daten

Neben der Datenerhebung und -verarbeitung durch Games-Unternehmen als Verantwortliche zu eigenen Zwecken, werden personenbezogene Daten ihrer Nutzer*innen aus unterschiedlichen Gründen auch weitergegeben. Den häufigsten Fall einer Datenweitergabe stellt meist die unternehmens- oder konzerninterne Weitergabe an die für die jeweilige Verarbeitung zuständige Abteilung wie die Finanzbuchhaltung, die Rechtsabteilung und den Konzerndatenschutz dar.[18] Ein typisches Bestreben im Konzern ist darüber hinaus die Nutzung von Synergieeffekten besonders im Bereich der Kundengewinnung oder des Cross-Marketings. In diesem Rahmen spielen Newsletterdaten häufig eine besondere Bedeutung in der Planung und Durchführung solcher Marketingmaßnahmen.[19] Daneben erfolgt die Datenweitergabe typischerweise entweder i.R.v. Auftragsverarbeitungen, wobei diese hier klar von gemeinsamen Datenverarbeitungen zu trennen sind. Ein besonders relevantes Problem stellt derzeit die grenzüberschreitende Datenweitergabe in Drittstaaten wie die USA oder mittlerweile auch das Vereinigte Königreich dar.

12 Als Drittanbieter werden z.B. häufig Crashlytics oder Firebase genutzt.
13 Als Drittanbieter werden z.B. häufig Kount, Riskified oder Signifyd genutzt.
14 Als Drittanbieter werden z.B. häufig Akismet, Captcha oder Cleantalk genutzt.
15 *EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel* – Planet49; *BGH* MMR 2020, 609 m. Anm. *Gierschmann* – Cookie-Einwilligung II; zu den Anforderungen an Cookie-Banner s.a. *Haberer*, MMR 2020, 810 und *Sesing*, MMR 2021, 547.
16 Hierzu ausf. *BGH* MMR 2020, 609 m. Anm. *Gierschmann* – Cookie-Einwilligung II.
17 So z.B. Firefox, Apple Safari und ab 2022 auch Chrome.
18 Bei einer einheitlichen Konzerndatenbank ist jederzeit der Trennungsgrundsatz aus Art. 5 Abs. 1 lit. b DS-GVO („Zweckbindung") zu beachten.
19 Zur Behandlung von Newsletter-Datenbanken in Games-Konzernen und den rechtlichen Voraussetzungen des Versands an Kund*innen anderer Konzernunternehmen sowie den erheblichen Problemen bei der Durchführung von Löschungs- und Abmeldeersuchen siehe in dieser Beilage *Bodensiek/Hoffmann*.

1. Typische Auftragsdatenverarbeitungen in Games-Unternehmen

Viele Games-Unternehmen beauftragen wie alle anderen Unternehmen auch ausgewählte externe Dienstleister wie z.B. Rechenzentren oder Plattformen für den Versand von Newslettern oder zur Einbindung von Bezahlmethoden. Oft werden auch Dienstleister genutzt, die die Beurteilung eines Werbekampagnenerfolgs ermöglichen oder bei der Vermeidung von Betrugsversuchen und Regelverstößen unterstützen sollen. Eine Auftragsdatenverarbeitung i.S.v. Art. 28 DS-GVO liegt in diesen Fällen nach einem Kurzpapier der unabhängigen Datenschutzbehörde des Bundes und der Länder (*Datenschutzkonferenz – DSK*) insbesondere dann vor, wenn in diesem Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten besteht. Sofern also die IP-Adresse der Nutzer*innen gekürzt und anonymisiert und dadurch der Personenbezug der IP-Adresse entfernt wird, liegt mangels Personenbezug keine Auftragsverarbeitung vor. Dies ist bei Abrechnungszwecken sicherlich sinnvoll. Gameplay-Daten der Spieler*innen werden in der Regel von Games-Unternehmen allerdings nicht weitergegeben, weil das Balancing quasi das Geschäftsgeheimnis eines jeden Anbieters ist.

2. Gemeinsame Datenverarbeitungen

Bei Games auf sozialen Netzwerken wie Facebook Instant Games und Snap Games Platform ist zu unterscheiden zwischen Games, die nur auf dem sozialen Netzwerk verfügbar und spielbar sind, und Games, bei denen ein Nutzer einen User-Account in einem sozialen Netzwerk haben muss. Nachdem der *EuGH*[20] für Facebook Fanpages entschieden hat, dass bei einer Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen, die die auf Facebook unterhaltenen Fanpages besucht haben, *Facebook* als „Verantwortlicher" anzusehen ist und damit eine gemeinsame Verantwortlichkeit („Joint-Controller") vorliegt, kann dies auch auf Games über soziale Plattformen übertragen werden. Spieleanbieter müssen demnach neben dem Impressum, einer eigenen Datenschutzerklärung und den Nutzungsbedingungen für das Spiel auch entsprechende Vereinbarungen mit den Plattformbetreibern abschließen. Mit Blick auf die Entscheidungen des *EuGH* in der Rs. Zeugen Jehovas[21] und Fashion ID[22] ist jedoch festzustellen, dass es für die gemeinsame Verantwortlichkeit noch keine klare Linie gibt.[23]

3. Datentransfers in Drittstaaten

Sofern bei gemeinsamen oder Auftragsdatenverarbeitungen grenzüberschreitende Verarbeitungen mit Drittstaaten vorgenommen werden, müssen ein Angemessenheitsbeschluss nach Art. 45 DS-GVO oder sonstige geeignete Garantien nach Art. 46 DS-GVO vorliegen. Ein solcher Angemessenheitsbeschluss ist nach dem Brexit und dem Ablauf der Übergangsfrist zum 1.7.2021 auch für das Vereinigte Königreich erforderlich. Insoweit könnte es sein, dass Games-Unternehmen zumindest übergangsweise Standardvertragsklauseln oder auch Binding Corporate Rules nutzen müssen. Gleiches gilt bereits für die USA, denn nach dem Urteil des *EuGH* in der Rs. Schrems II[24] ist der EU-US-Privacy-Shield keine ausreichende Grundlage für Datenübermittlungen in die USA. Games-Unternehmen bedienen sich allerdings schon jetzt weit überwiegend der Standardvertragsklauseln und ergreifen in Ergänzung technische und organisatorische Maßnahmen. Die *EU-Kommission* hat am 4.6.2021 neue Standardvertragsklauseln für den Drittstaatentransfer von Daten verabschiedet.[25] Die bisherigen Standardvertragsklauseln werden nach drei Monaten ab Inkrafttreten des neuen Klauselwerks aufgehoben. Bei Verträgen, die vor dem Datum der Aufhebung auf Basis der aktuellen Standardvertragsklauseln geschlossen wurden, gilt eine weitere Übergangsfrist von 15 Monaten, in der der Datentransfer auf Basis der bisherigen Standardvertragsklauseln erfolgen kann.

VI. Fazit: Same same, but different

Nach drei Jahren DS-GVO hat die Games-Branche praktikable und auch kundenfreundliche Lösungen für den Datenschutz gefunden, die sich weitgehend bewährt haben. Anders als bei anderen Medienbranchen steht hierbei nicht das Tracking und Targeting für Werbung durch Dritte im Vordergrund. Es geht vielmehr um die Verbesserung des Spielerlebnisses und um maßgeschneiderte Angebote zum Spiel. Dies ist regelmäßig durch die berechtigten Interessen gedeckt und auch Cookies sollten weiterhin bei dieser Verwendung als funktional betrachtet werden und daher keiner Einwilligung bedürfen. I.E. ist die DS-GVO wegen der europaweiten Rechtsvereinheitlichung für Games, die europaweit vertrieben werden, ein großer Gewinn. Hinderlich ist allerdings noch die nicht gefestigte Auslegung der einheitlichen Normen. Dies zeigt sich insbesondere bei der Aufsicht, die in diesem Beitrag nicht weiter thematisiert wurde, auf die aber *Moos* in dieser Beilage ausführlich eingeht. Bei der Anwendung der bestehenden Normen und den anstehenden Reformen mit der ePrivacy-VO und dem Data Act wird sich zeigen, ob die besonderen Bedürfnisse und Funktionsweisen der Games-Branche verstanden und berücksichtigt werden.

Schnell gelesen ...

- Es gibt viele verschiedene Kategorien von Daten bei Computerspielen, die gesammelt werden, jedoch weniger um Werbung, sondern das Spielerlebnis zu unterstützen.
- Die meisten Datenverarbeitungen erfolgen auf der Grundlage des Nutzungsvertrags und teilweise auch aus berechtigten Interessen, während die Einwilligung eher die Ausnahme darstellt.
- Tracking und Cookies werden vielfach für das plattformübergreifende Spielen und zur Verbesserung des Spielerlebnisses genutzt, in der Regel nicht für die passgenaue Werbung durch Dritte.
- Datentransfers in Drittstaaten erfolgen vor allem auf der Grundlage der Standardvertragsklauseln, insbesondere weil die Daten weltweit geteilt werden müssen.

Jürgen Bänsch
ist Director, Policy & Public Affairs bei der Interactive Software Federation of Europe (ISFE) – der Verband der europäischen Games-Branche in Brüssel.

Professor Dr. Christian-Henner Hentsch, M.A., LL.M.,
ist Leiter Recht & Regulierung beim game – Verband der deutschen Games-Branche in Berlin, Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln und Mitherausgeber der MMR.

20 *EuGH* MMR 2018, 591 m. Anm. *Moos/Rothkegel* – Facebook-Fanpages.
21 *EuGH* ZD 2018, 469 m. Anm. *Hoeren* – Zeugen Jehovas.
22 *EuGH* MMR 2019, 579 m. Anm. *Moos/Rothkegel* = ZD 2019, 455 m. Anm. *Hanloser* – Fashion ID.
23 Ausf. zum Datenschutz bei Games auf sozialen Netzwerken siehe in dieser Beilage *Lober/Klein.*
24 *EuGH* MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel* – Schrems II.
25 S. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

PATRICK MITSCHING / CHRISTIAN RAUDA

Zeitenwende beim Tracking des Nutzungsverhaltens durch Spiele-Apps

Benutzer- und Gerätedaten

Bedeutung von Apples App Tracking Transparency Framework (ATT-Framework) für Spiele-Entwicklerstudios aus datenschutzrechtlicher Perspektive

Der Beitrag widmet sich der datenschutzrechtlichen Einordnung des im April 2021 auf Apple-Geräten ab iOS 14.5 eingeführten App Tracking Transparency-Framework (ATT-Framework). Obgleich Apple kein Gesetzgeber und das ATT-Framework kein Gesetz ist, stellt ATT doch eine faktisch Rechtssetzung mittels globaler Plattform-AGB gegenüber Spiele-Entwicklerstudios und Spieler*innen dar. Erstmalig wird für mobile Endgeräte eines Herstellers ein unumgänglicher Mechanismus geschaffen, um von Spieler*innen die Erlaubnis für das Tracking über die Spiel-App hinaus in anderen Apps und Websites einzuholen. Dies hat weitreichende Folgen vor allem für die Bewerbung und Monetarisierung von Spiele-Apps, die auf Tracking angewiesen sind. Lesedauer: 18 Minuten

I. Einleitung

Apple hat die Welt der App-Entwicklerstudios ins Wanken gebracht. In den Betriebssystemen iOS 6 bis iOS 13 hatten sie freien Zugriff auf die eindeutige Werbe-ID des Apple-Geräts (IDFA). Die IDFA ist eine jedem Apple-Gerät innewohnende eindeutige und weltweit gültige Identifikationsnummer bestehend aus 32 Zeichen (z.B. EA7583CD-A667-48BC-B806-42ECB2B48606). Der Nutzer hatte die Möglichkeit, den Zugriff durch Modifikationen in den Datenschutzeinstellungen zu ändern und konnte zunächst die IDFA zurücksetzen oder sperren. Seit iOS 14 war ein Zurücksetzen nicht mehr möglich, man konnte den Zugriff auf die IDFA allerdings manuell ganz sperren, indem man den Menüpunkt „Apps erlauben, Tracking anzufordern" deaktivierte. Viele Nutzer*innen hatten von dieser Option allerdings keine Kenntnis. Dies führte dazu, dass die Mehrheit der Nutzer*innen ohne Weiteres „trackbar" waren. *Apple* hat nun die Möglichkeit des Trackings eingeschränkt und dafür viel Lob von Datenschützer*innen geerntet, sich aber auch viel Kritik ausgesetzt. Unter der Flagge des Datenschutzes verfolgt *Apple* nämlich durchaus eigene wirtschaftliche Interessen.

II. App Tracking Transparency Framework

Mit dem Update des Betriebssystems iOS auf die Version 14.5 am 26.4.2021 wurde das sog. App Tracking Transparency Framework (ATT-Framework) eingeführt. *Apple* schreibt nun vor, dass App-Entwicklerstudios das ATT-Framework verwenden müssen, wenn ihre App Daten über Endbenutzer*innen sammeln und diese mit anderen Unternehmen zum Zweck des Trackings über Apps und Websites hinweg teilen. Dieses Zusammenführen geschieht regelmäßig in zwei Fällen: Wenn der App-Entwickler bei einem digitalen Werbeunternehmen Werbung für seine eigene App schaltet (Nutzergewinnung). Oder wenn der App-Entwickler Werbefläche in seiner App an Werbeunternehmen gegen Entgelt zur Verfügung stellt (Werbevermarktung). In beiden Fällen tauschen der App-Entwickler und das Werbeunternehmen die IDFA erfolgreich geworbener Nutzer*innen aus (Attribution). Dies ermöglicht eine klare Messung und Vergütung des Werbeerfolgs. Es wird i.Ü. Betrug verhindert. Andernfalls bestünde die Gefahr, dass der App-Entwickler für die Gewinnung von fiktiven Nutzer*innen bezahlt, also Nutzer*innen, die ihm durch das Werbeunternehmen gar nicht zugeführt wurden (Werbebetrug).

III. Was ist für Apple „Tracking"?

Unter „Tracking" versteht *Apple* die Verknüpfung von Benutzer- oder Gerätedaten, die von den Apps, Websites oder Offline-Eigenschaften anderer Unternehmen gesammelt wurden, um gezielte Werbung oder Werbemessung zu betreiben. Tracking bezieht sich auch auf die Weitergabe von Benutzer- oder Gerätedaten an Datenbroker[1]. *Apple* nennt auch Beispiele für Tracking, nämlich

- Anzeigen von gezielter Werbung in der App, die auf Benutzerdaten basiert, die von Apps und Websites anderer Unternehmen gesammelt wurden.
- Teilen von Gerätestandortdaten oder E-Mail-Listen mit einem Datenbroker.
- Weitergabe einer Liste von E-Mails, Werbe-IDs oder anderen IDs an ein Werbenetzwerk eines Drittanbieters, das diese Informationen verwendet, um diese Nutzer*innen in den Apps anderer Entwickler erneut anzusprechen oder ähnliche Benutzer*innen zu finden.
- Platzieren eines Software Development Kit (SDK) eines Drittanbieters in der App, das Nutzerdaten aus der App mit Nutzerdaten aus den Apps anderer App-Entwickler kombiniert, um Werbung gezielt zu platzieren oder die Werbeeffizienz zu messen, auch wenn das SDK nicht für diese Zwecke verwendet wird.

Nicht als Tracking eingeordnet wird dagegen, wenn Benutzer- oder Gerätedaten aus der App ausschließlich auf dem Gerät der Nutzer*innen mit Daten Dritter verknüpft werden und nicht auf eine Weise vom Gerät gesendet werden, die die Nutzer*innen oder das Gerät identifizieren kann oder wenn ein Datenbroker, mit dem Daten geteilt werden, die Daten ausschließlich zur Betrugserkennung, Betrugsprävention oder zu Sicherheitszwecken und ausschließlich im Namen des App-Entwicklers verwendet.

IV. Implementierung des ATT-Framework

Technisch setzt die Implementierung des ATT-Framework voraus, dass App-Entwicklerstudios einen von *Apple* vorgegebenen und für alle Apps einheitlichen Programmcode in ihre App einbauen. Dieser Code führt beim Start der App zur Anzeige eines Systemdialogs („ATT-Prompt"). In diesem ATT-Prompt wird der Nutzer um Erlaubnis dafür gebeten, dass „die App ihre Aktivitä-

1 https://developer.apple.com/app-store/user-privacy-and-data-use/.

ten in Apps und auf den Websites anderen Unternehmen erfassen" darf. Außerdem muss vom App-Entwickler eine Beschreibung des Grunds für das Tracking angezeigt werden (usage-description string). Die Nutzer*innen der App sind frei darin, ob sie die Erlaubnis erteilen oder nicht. *Apple* weist darauf hin, dass die App beim ersten Start durch einen Nutzer abstürzen kann, sofern kein usage-description string implementiert ist. Nachdem der Nutzer die Erlaubnis erteilt oder verweigert hat, speichert die App dies (Tracking-Autorisierungsstatus). Der App-Entwickler hat insofern nur einen „Schuss", um eine Erlaubnis zu erhalten. Dies hat dazu geführt, dass viele App-Entwickler nach Einführung des ATT-Framework erst einmal abgewartet haben und zunächst kein ATT-Prompt aktiviert haben.[2] Wenn der Nutzer der App ihre Erlaubnis nicht gibt, kann der App-Entwickler nicht erneut um Erlaubnis fragen. Der Nutzer muss vielmehr in den Systemeinstellungen aktiv die Erlaubnis zu Gunsten des App-Entwicklers erteilen. *Apple* verbietet es App-Entwickler, die Regelung des „einen Schusses" zu umgehen. So ist es etwa verboten, dem nativen ATT-Prompt ein eigenes Fenster vorzuschalten, in dem die Nutzer*innen „Ich entscheide mich später" auswählen und so die Entscheidung zurückstellen können. Auch ist es verboten, die Nutzung der App an die Erteilung der Erlaubnis zu koppeln (gating) oder durch Anreize wie z.B. Gratisleistungen oder Rabatte die Erteilung der Erlaubnis attraktiver zu gestalten (incentivization).[3]

Für Nutzer*innen gibt es wenig erkennbare Anreize, einem Tracking zuzustimmen. Vielen Nutzer*innen ist nicht einmal klar, dass es einen Unterschied zwischen Tracking im Internet und dem Anzeigen von Werbung gibt. Die Verweigerung der Erlaubnis in das Tracking verhindert nämlich natürlich nicht, dass den Nutzer*innen Werbung angezeigt wird. Ohne Tracking ist die angezeigte Werbung nur nicht mehr auf die Nutzer*innen zugeschnitten. Dies kann z.B. dazu führen, dass Veganer*innen Fleischprodukte angeboten werden oder Männern Hygieneartikel für Frauen. Dass Tracking also auch Vorteile für die Nutzer*innen hat, ist kaum jemandem klar. Dies führt dazu, dass viele die Erlaubnis verweigern werden. Historisch betrachtet waren vor der ATT-Einführung im April 2021 ca. 90% aller IDFA frei verfügbar, da nur wenige Nutzer*innen das Tracking in den Systemeinstellungen deaktivierten. Neueste Erhebungen seit der ATT-Einführung ab Juni 2021 deuten darauf hin, dass sich die effektive IDFA-Verfügbarkeitsquote abhängig von App-Kategorie und geografischer Region bei 15 bis 20% oder weniger einpendelt.[4] Die Folge davon für die App-Entwickler sind hohe Streuverluste bei der Nutzergewinnung und sinkende Werbeeinnahmen bei der Werbevermarktung. Denn der Vorteil von Online-Werbung gegenüber etwa Außen- oder Fernsehwerbung liegt darin, dass die Zielgruppe viel genauer identifiziert und angesprochen werden kann. Damit werden Streuverluste minimiert und die Bereitschaft der Hersteller und Händler erhöht, hohe Preise für gezielte Werbung auszugeben. Die mit Abstand größten Werbeunternehmen *Facebook* und *Google* behaupten, dass die Einnahmen von Werbeflächenanbietern – hier: App-Entwicklern – ohne personalisierte Werbung um 50% (Angabe von *Facebook*) bzw. 52-64% (Angabe von *Google*) zurückgehen würden.[5] Diese Größenordnung wird auch von deutschen Werbeverbänden in deren aktueller ATT-Kartellbeschwerde gegen *Apple* vor dem *Bundeskartellamt* angeführt.[6] Allerdings ist zu beachten, dass unabhängige empirische Studien einen deutlich geringeren Rückgang der Einnahmen prognostizieren, nämlich um nur ca. 4%.[7] Spiele-Entwicklerstudios, die in ihren Spielen überwiegend nur noch Werbung anbieten können, welche nicht auf die Interessen des Nutzers zugeschnitten sind, erlösen also weniger Werbeeinnahmen.

V. Datenschutzrechtliche Einordnung

1. Einordnung der ATT-Erlaubnis als Einwilligung

Ob es sich bei der von dem Entwickler über das ATT-Framework erbetene „Erlaubnis" um eine Einwilligung im datenschutzrechtlichen Sinne handelt, ist umstritten. Die Frage hat Relevanz für das Ausspielen von Werbung an Nutzer*innen auf anderen Geräten und Plattformen, insbesondere solchen außerhalb von *Apples* digitalem Ökosystem.

Nach der Einwilligungs-Theorie kann es sich bei der angeforderten Erlaubnis um eine Einwilligung i.S.d. Art. 6 Abs. 1 lit. a DS-GVO handeln, die sich insgesamt auf die Befugnis zum Tracking durch den App-Entwickler bezieht.[8] Demnach messen die Nutzer*innen dem ATT-Prompt eine rechtliche Qualität zu und entscheiden gegenüber dem App-Entwickler, ob sie mit einem Tracking über alle Geräte und Plattformen hinweg einverstanden sind, auf denen das Spiel angeboten wird. Dafür spricht, dass *Apple* in seiner ATT-Richtline der Entscheidung des Nutzers über Erlaubnis oder Verweigerung des Trackings eine sehr umfassende Geltung beimisst, die sich abstrakt auf die „App" als universelles Produkt bezieht, welche auf verschiedenen Geräten und Plattformen genutzt werden kann.[9]

Die Gegenmeinung vertritt die Gerätespezifische Theorie. Danach handele es sich bei der Erteilung oder Verweigerung der Erlaubnis um eine reine Geräteeinstellung, die keine allgemeine Rechtsqualität aufweist und damit auch keine Rechtswirkung gegenüber dem App-Entwickler entfaltet.[10] Die Nutzer*innen verstünden das ATT-Prompt als reine Abfrage einer nur für dieses eine Gerät gültigen Systemeinstellung. Eine DS-GVO-konforme Einwilligung liege nicht vor, weil schon die Aufklärungspflichten aus Art. 7 DS-GVO nicht erfüllt seien, da im ATT-Prompt nicht auf die Datenschutzerklärung verlinkt werden kann.[11] Die Nutzer*innen verbieten damit dem App-Entwickler nicht das Tracking jenseits des konkreten *Apple*-Geräts, auf dem die Einstellung vorgenommen werde.

Welcher Meinung man folgt, hat weitereichende Konsequenzen in Bezug auf Spiele, die auf mehreren Geräten und Plattformen gespielt werden können (Cross-Plattform-Spiele). Cross-Plattform-Spiele zeichnen sich dadurch aus, dass sie auf unterschiedlichen Endgeräten und Betriebssystemen genutzt werden

2 https://www.businessinsider.com/why-you-are-not-seeing-ios-145-privacy-pop-ups-2021-4; https://www.fastcompany.com/90632354/ios-14-5-privacy-pop-up-requests-not-showing-up.

3 S. Fußn. 1.

4 *Flurry*: 15%, abrufbar unter: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/; *Singular*: 20%, abrufbar unter: https://www.singular.net/blog/ios-14-5-by-the-numbers-adoption-att-permission-ad-spend-trends-install-volume-impact-on-android-vs-ios/.

5 *Facebook*: -50%, abrufbar unter: https://developers.facebook.com/blog/post/2020/06/18/value-of-personalized-ads-thriving-app-ecosystem/; *Google*: -52-64%, abrufbar unter: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf.

6 *Pettinger*, Zwingt Apples Datenschutz Unternehmen in die Knie?, abrufbar unter: https://www.dr-datenschutz.de/zwingt-apples-datenschutz-unternehmen-in-die-knie/.

7 *Marotta* et al., Online Tracking and Publisher's Revenues: An Empirical Analysis, abrufbar unter: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

8 *Obereck/Frank*, iOS 14.5 – Apple gibt Nutzern Wahlrecht bei App-Tracking, abrufbar unter: https://www.datenschutzkanzlei.de/ios-14-5-apple-gibt-nutzern-wahlrecht-bei-app-tracking/; *Isaacson*, Apple iOS14 Changes: „Your App" May No Longer Mean „Your Data", abrufbar unter: https://www.adexchanger.com/data-driven-thinking/apple-ios14-changes-your-app-may-no-longer-mean-your-data-2/.

9 S. Fußn. 1.

10 Apples ATT: Was es bedeutet, wenn kaum einer Tracking will, abrufbar unter: https://www.dr-datenschutz.de/apples-att-was-es-bedeutet-wenn-kaum-einer-tracking-will; *McChannel*, Be Cautious App Developers: ATT and GDPR are not the same, abrufbar unter: https://appgrowthsummit.com/be-cautious-app-developers-att-and-gdpr-are-not-the-same/.

11 S. Fußn. 10.

können. Wer also ein Spiel mobil im Zug gespielt hat, kann nach der Ankunft zuhause dieselbe Partie nahtlos auf dem heimischen PC weiterspielen. Spielt ein Nutzer das Cross-Plattform-Spiel „Forge of Empires" auf seinem iPhone, iPad und PC, kann die Tracking-Erlaubnis durchaus auseinanderfallen. Für das iPhone hat er etwa das Tracking abgelehnt, für das iPad hat er das Tracking akzeptiert und für den PC wurde er zum Tracking gar nicht gefragt, da dieser nicht das Betriebssystem iOS nutzt und somit dort das ATT-Framework nicht existiert.

Für die Gerätespezifische Theorie spricht, dass Nutzer*innen bei der Auswahl im ATT-Prompt nur das konkrete Gerät vor Augen haben, das sie gerade nutzen. Sie machen sich keine Vorstellungen darüber, ob die Erlaubnis irgendeine Auswirkung auf die Nutzung des Spiels auf anderen Geräten oder Plattformen haben könnte. Eine andere Ansicht ist praxisfern und konstruiert einen Rechtswillen, den die Nutzer*innen nicht haben. Allerdings missversteht die Gerätespezifische Theorie, dass der Nutzerentscheidung sehr wohl eine Rechtsqualität bezogen auf das betroffene Gerät innewohnt: Die Nutzer*innen bringen durch ihre Auswahl im ATT-Prompt zum Ausdruck, dass sie mit Tracking einverstanden oder nicht einverstanden sind. Die Abfrage im ATT-Prompt geschieht in bewusst einfacher und klarer Sprache, so wie es u.a. Erwägungsgrund 58 DS-GVO erfordert. Die Datenschutzerklärung können die Nutzer*innen unkompliziert vor oder während der Installation auf der App-Store-Seite der App nachlesen. An den Inhalt und Umfang des ATT-Prompts sollten insofern keine überzogenen Forderungen gestellt werden – das ATT-Prompt ist deutlich und warnend. Überzeugend ist es daher, die Gerätespezifische Theorie so zu modifizieren, dass sie eine gerätebezogene Einwilligung im ATT-Prompt ermöglicht.

Unter datenschutzrechtlichen Gesichtspunkten ist die Implementierung einer solchen dem Tracking vorgeschalteten Erlaubnis mit Einwilligungscharakter zu begrüßen.

2. Einordnung der IDFA als personenbezogenes Datum nach DS-GVO

Die IDFA ermöglicht die Verknüpfung mit weiteren personenbezogenen Daten, durch die ein Personenbezug hergestellt werden kann, nicht jedoch mit dauerhaft dem Gerät zugeordneten Daten.[12] In der Praxis ist die IDFA in ihrer Funktion einem Cookie sehr ähnlich: Der im Browser gesetzte Cookie erlaubt ebenso wie die im iOS-Betriebssystem vergebene IDFA eine Nachverfolgung des Nutzerverhaltens. So wie der Cookie die von Nutzer*innen aufgerufenen Websites und dortigen Eingaben protokolliert, werden anhand der IDFA die von Nutzer*innen aufgerufenen Apps und Websites und darin getätigten Handlungen protokolliert. Ein technischer Unterschied besteht nur darin, dass der Cookie manuell vom Website-Anbieter in den Quellcode seiner Website eingebunden werden muss, während die IDFA bereits im iOS-Gerät ab Werk vorhanden ist. Letztlich werden die aus Cookie-Setzung und IDFA-Zuordnungen erhobenen Daten gleichrangig wie Wirtschaftsgüter gehandelt: Ein Website- oder App-Anbieter, der Trackingdaten zu Nutzungs- und Kaufverhalten liefern kann, erhält von Werbeunternehmen eine erheblich höhere Werbevergütung als ein Anbieter, der keine Trackingdaten bereitstellen kann oder will. In der Werbebranche werden Cookies und IDFA einheitlich als „audience identifiers" behandelt, wobei Cookies für den Bereich „Web" und IDFA für den Bereich „Non-Web" relevant sind.[13]

Es ist immer noch umstritten, ob die IDFA als personenbezogenes Datum unter der DS-GVO einzuordnen ist. Erwägungsgrund 30 DS-GVO legt fest, dass Personen „unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet" werden. Dies könne dann „Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren". Zwar konnte man die IDFA zunächst zurücksetzen oder deaktivieren und seit iOS 13 ausschalten (Limited Ad Tracking – LAT). Wird dies indes nicht getan, spricht viel dafür, die IDFA als personenbezogenes Datum anzusehen.[14]

3. Einordnung der IDFA als geschützte Information nach ePrivacy-RL

Nachdem der *EuGH* in der Rs. Planet49[15] entschieden hat, dass bei der Nutzung von Cookies auf Webseiten grundsätzlich eine Einwilligung erforderlich ist, stellt sich natürlich die Frage, wie dies bei anderen Tracking-Technologien zu beurteilen ist. Die IDFA ist praktisch für iOS-Mobilgeräte das, was Cookies für Websites sind. Cookies waren deswegen jahrelang so umstritten, weil durch sie Tracking von Nutzer*innen beim Surfen von Website zu Website möglich wurde, was wiederum Profilbildung und damit gezielte Werbung ermöglichte. Bei Mobilgeräten ersetzen Werbe-IDs (u.a. IDFA) die dort technisch bedingt nicht vorhandenen Cookies praktisch vollständig und ermöglichen das Tracking von Nutzer*innen bei Interaktion in den verschiedenen Apps und Websites, sodass auch dort Profilbildung und gezielte Werbung möglich werden. Als Faustregel gilt, dass man bei der Nutzung solcher Technologien immer dann eine Einwilligung braucht, wenn dies nach der ePrivacy-Richtlinie (ePrivacy-RL) vorgesehen ist.

Art. 5 Abs. 3 ePrivacy-RL befasst sich mit der „Speicherung von Informationen oder dem Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind." Es muss sichergestellt sein, dass Nutzer*innen auf die Möglichkeit hingewiesen werden, diese Verarbeitung zu verweigern. In der Planet49-Entscheidung macht der *EuGH* deutlich, dass das Einwilligungserfordernis in Art. 5 Abs. 3 S. 1 ePrivacy-RL unabhängig davon gelte, ob es sich bei den in einem Cookie gespeicherten Informationen um personenbezogene oder um anonyme Daten handele. Auch Art. 5 Abs. 2 ePrivacy-RL setze nicht voraus, dass sich die Speicherung oder der Zugriff auf personenbezogene Daten beziehen müsse.[16] Es gehe um den Schutz von sämtlichen in Endgeräten von Nutzer*innen gespeicherte Informationen, ohne dass dabei zwischen personenbezogenen und anderen Informationen zu differenzieren sei.[17]

Da die IDFA im Gerät des Nutzers gespeichert wird, bedarf es also einer Einwilligung. In diesem Zusammenhang ist auch zu beachten, dass der *Bundestag* am 20.5.2021 den Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) verabschiedet hat. § 25 TTSDG-E soll Art. 5 Abs. 3 ePrivacy-RL umsetzen. Nach der Vorschrift soll die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig sein, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Regelung orientiert sich unmittelbar am Wortlaut der europäischen Vorgaben.[18] § 25 TTDSG-E soll laut der Begründung des Regierungsentwurfs indes nur auf nicht-perso-

12 *Koreng/Lachenmann*, Formularhdb. Datenschutzrecht, 2018, F. I. 2. Rn. 7.
13 https://support.google.com/admanager/answer/6280452?hl=en.
14 *Weichert*, SVR 2014, 201 (204); *Hoffmann*, MMR 2013, 631 (634).
15 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
16 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
17 *EuGH* MMR 2019, 736 m. Anm. *Moos/Rothkegel* – Planet49.
18 *Schwartmann/Benedikt/Reif*, MMR 2021, 99.

nenbezogene Daten Anwendung finden, in Bezug auf personenbezogene Daten sei die DS-GVO einschlägig.

VI. Kritik am ATT-Framework

Die Einführung von *Apples* ATT-Framework wurde u.a. von *Facebook* und Werbeverbänden stark und öffentlichkeitswirksam kritisiert mit dem Argument, dass *Apple* die Entwickler von Apps dazu zwinge, von Werbung auf Abomodelle und In-App-Käufe umzustellen, an denen *Apple* mitverdient. In Frankreich legten die Werbeverbände eine Beschwerde bei der Kartellbehörde ein, die jedoch erfolglos blieb.[19] In Deutschland legten die Werbeverbände ebenfalls Beschwerde beim *Bundeskartellamt* ein, über die zum Zeitpunkt der Schriftlegung noch nicht entschieden ist.[20] *Apple* erhebt auf alle im App-Store im B2C-Verhältnis erworbenen Abos und In-App-Käufe mit wenigen Ausnahmen eine Gebühr von 30% des Transaktionsvolumens. Demgegenüber profitiert *Apple* von werbefinanzierten Apps nicht, da die Werbevergütung im B2B-Verhältnis zwischen App-Entwickler und Werbeanbieter außerhalb des App-Stores abgewickelt wird.[21] Zudem wird *Apple* vorgeworfen, selbst verstärkt Werbeplätze in den Suchergebnislisten im App-Store verkaufen zu wollen, analog zu *Googles* erfolgreichen Werbeplätzen neben den Suchergebnissen bei Google Search.[22] *Apple* gehe es also im Kern nicht um den Datenschutz, sondern um die Erhöhung der eigenen Umsätze und die Ausweitung seiner Kontrolle über die App-Entwickler.

Apple hat nämlich parallel zur ATT-Einführung seine eigenen Werbeflächen im App-Store stark ausgebaut.[23] Dort verarbeitet *Apple* die im eigenen iOS-Ökosystem erhobenen First-Party-Daten für Werbeplätze, die Dritte buchen können. Eine gezielte Ansprache einzelner Nutzer*innen ist zwar nicht möglich, allerdings eine Ansprache von Kohorten ab 5.000 Personen, bei denen die Einzelpersonen ähnliche Merkmale aufweisen.[24] Somit wird letztlich das individuelle Tracking durch ein neues Kohorten-Tracking ersetzt. Noch anspruchsvollere Ansätze sind die AI-basierte Auswertung von Nutzerverhalten mittels „Differential Privacy" und „Federated Learning", die etwa bei der Personalisierung von *Apples* Sprachassistent Siri eingesetzt werden.[25] Zu beachten ist allerdings, dass auch ein solches Kohorten-Tracking der DS-GVO unterliegt, solange Daten in diesem Rahmen auf einzelne Personen rückbezogen werden können. Da *Apple* diesen „Datenschatz" mit niemandem teilen muss, ist er besonders wertvoll. Sog. „First-Party-Tracking" ist gegenüber „Third-Party-Tracking" privilegiert.[26] *Schwartmann* bezeichnete *Apple* daher als „selbsternannten Zöllner mit Eigeninteressen"[27].

VII. Fazit

Die Spiele-Entwicklerstudios müssen ihre Herangehensweise bei der Nutzergewinnung und Werbevermarktung innovativ verändern. Der Trend geht dahin, nicht mehr das Verhalten einzelner Nutzer*innen zu erfassen, sondern auf der Ebene von Nutzergruppen mit gemeinsamen Merkmalen (Kohorten) aggregierte Daten zu erheben. Zudem ist eine Abkehr vom Tracking anhand deterministischer Marker wie Werbe-IDs hin zu Annahmen auf Grund probabilistischer Marker wie Gerätetyp, Nutzungszeitpunkt und Werbekontext zu erwarten. Parallel wird der Wert von First-Party-Daten bei Entwicklerstudios und Werbeunternehmen zunehmen, da Third-Party-Daten auf Grund fehlender Tracking-Einwilligungen nicht mehr beliebig erhoben und ausgetauscht werden können. Dies wird zu verstärkter vertikaler Integration von Entwicklerstudios und Werbeunternehmen führen, um einen gemeinsamen Bestand an First-Party-Daten aufzubauen. Die weitere Entwicklung wird auch Aufschluss darüber geben, wie abhängig Spiele-Entwicklerstudios und Werbewirtschaft tatsächlich vom Tracking individueller Nutzer*innen sind.

Schnell gelesen ...

- Unter „Tracking" versteht Apple die Verknüpfung von Benutzer- oder Gerätedaten, die von den Apps, Websites oder Offline-Eigenschaften anderer Unternehmen gesammelt wurden, um gezielte Werbung oder Werbemessung zu betreiben.
- Der App-Entwickler muss einen von Apple vorgegebenen und für alle Apps einheitlichen Programmcode (App Tracking Transparency Framework – ATT-Framework) in seine App einbauen. Durch diesen wird eine Erlaubnis zum Tracking abgefragt. Die effektive Erlaubnisrate zum Tracking bei Spiele-Apps liegt inzwischen nur noch bei ca. 15-20%. Die Folge davon für die Spiele-Entwicklerstudios sind hohe Streuverluste bei der Nutzergewinnung und sinkende Werbeeinnahmen bei der Werbevermarktung.
- Bei der Erteilung der Erlaubnis handelt es sich um eine auf das konkrete Apple-Gerät bezogene Einwilligung. Sie erfüllt indes nicht die Voraussetzungen einer für alle Geräte und Plattformen gültigen allgemeinen Einwilligung gegenüber dem Spiele-Entwicklerstudio. Diese Unterscheidung ist wichtig für Cross-Plattform-Spiele. Da die IDFA im Gerät des Nutzers gespeichert wird, bedarf es nach Art. 5 Abs. 3 ePrivacy-RL einer Einwilligung.
- Die Spiele-Entwicklerstudios müssen ihre Herangehensweise bei der Nutzergewinnung und Werbevermarktung innovativ verändern. Der Trend geht dahin, nicht mehr das Verhalten einzelner Nutzer*innen zu erfassen, sondern auf der Ebene von Nutzergruppen mit gemeinsamen Merkmalen (Kohorten) aggregierte Daten zu erheben. Zudem steigt die Bedeutung von probabilistischen Daten und First-Party-Daten.

Patrick Mitsching, LL.M. (Durham), M.A. (London),
ist Leiter der Rechtsabteilung bei der InnoGames GmbH in Hamburg.

RA Dr. Christian Rauda
ist Fachanwalt für Informationstechnologierecht, für Urheber- und Medienrecht und für gewerblichen Rechtsschutz und Partner der Medienrechtskanzlei GRAEF Rechtsanwälte (Hamburg/Berlin) sowie Lehrbeauftragter an der Bucerius Law School und der Hochschule für Technik und Wirtschaft Berlin.

19 https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-solicitation-autorite-does-not-issue.
20 https://zaw.de/missbrauchsbeschwerde-der-medien-und-werbewirtschaft-gegen-apple-beim-bundeskartellamt/.
21 S. Fußn. 20.
22 S. Fußn. 20.
23 https://9to5mac.com/2021/05/04/apple-emails-search-ads-app-store/.
24 https://searchads.apple.com/help/advanced/0021-set-campaign-refinements/.
25 *Hao*, How Apple personalizes Siri without hovering up your data, abrufbar unter: https://www.technologyreview.com/2019/12/11/131629/apple-ai-personalizes-siri-federated-learning/; *Ippolito*, AI Differential Privacy and Federated Learning, abrufbar unter. https://towardsdatascience.com/ai-differential-privacy-and-federated-learning-523146d46b85; https://machinelearning.apple.com/research/learning-with-privacy-at-scale.
26 Dies sieht im Grundsatz auch die *Datenschutzkonferenz* so, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, S. 17.
27 FAZ v. 10.5.2021, S. 18.

KAI BODENSIEK / DAVID JULIAN HOFFMANN

Newsletter im Konzern – kein Selbstläufer!

Praxisbezogene Betrachtung des Umgangs mit Newsletter-Datenbanken

Newsletter-Marketing

Der Beitrag befasst sich mit den besonderen rechtlichen und tatsächlichen Problemen des Newsletter-Versands vom Beginn des Newsletter-Abonnements bis zu dessen Ende. Dabei werden die unterschiedlichen Arten und Formen der Newsletter betrachtet und rechtlich eingeordnet. Ein Fokus liegt auf den üblichen Problemen beim Newsletter-Marketing in Unternehmensgruppen, die häufig bestrebt sind, Cross-Marketing-Effekte zu optimieren und einheitliche technische Strukturen zu schaffen. Schließlich ist die Games-Branche in stetiger Bewegung, auch Unternehmensübernahmen sind tägliche Normalität. Auch hieraus ergeben sich Probleme, z.B. bei der Integration bestehender Datenbanken in die Konzernstruktur nach einem Unternehmenskauf. Die sich ergebenden Probleme, insbesondere aus dem Bereich des Wettbewerbs- und des Datenschutzrechts, werden vor allem unter praktischen Gesichtspunkten beleuchtet. Lesedauer: 21 Minuten

I. Kundenansprache über das Internet

Das Internet wird gemeinhin – zu Recht – als bahnbrechende Erfindung betrachtet. Insbesondere ermöglicht das Internet per E-Mail eine direkte Kundenansprache, ohne dabei die sonst typischen Kosten und Zeitaufwände von Druck und Versand zu verursachen. Auch sind die Nachverfolgung und Reaktionen auf einen versendeten Newsletter technisch leicht umsetzbar.

Es liegt nahe, dass die Effizienz von Newslettern, auch auf Grund ihrer Allgegenwärtigkeit, nicht mehr so hoch ist, wie noch vor einigen Jahren. Auch sind die Verbraucher*innen seit der prominent durch die Medien begleiteten Einführung der DS-GVO deutlich datenschutz-affiner geworden. Trotzdem erfreut sich der Newsletter in den meisten Unternehmen immer noch großer Beliebtheit als beliebtes Kundenbindungs- und Akquirierungsinstrument. Unternehmen fast aller Branchen nutzen den Newsletter, um Kund*innen anzusprechen und ihre Produkte hervorzuheben.

Bei der Anstrengung von Unternehmen, eine möglichst große Anzahl von Kund*innen mit möglichst vielen Neuigkeiten per Newsletter anzusprechen, sollte auf jeden Fall nicht vernachlässigt werden, die notwendigen rechtlichen Rahmenbedingungen, vor allem auch die datenschutzrechtlichen Anforderungen, genau zu beachten. Besondere rechtliche Fragestellungen kommen auf, wenn der Newsletter-Versand innerhalb einer Konzerngruppe organisiert werden soll – oder wenn Newsletter-Bestände auch für Produkte anderer Konzernunternehmen nutzbar gemacht werden sollen.

II. Verschiedene Arten von Newslettern

Newsletter ist bekanntlich nicht gleich Newsletter. Es gibt verschiedene Arten von Newslettern – den Inhalt, aber auch den Absender betreffend – und damit auch keine einheitliche und allgemeingültige Rechtsgrundlage für deren Versand. Im Wesentlichen gibt es den Produkt-Newsletter, den Unternehmens-Newsletter und – bei Konzernen – den Konzern-Newsletter.

1. Produkt-Newsletter

Der Standardfall des Produkt-Newsletters ist der, dass ein Kunde ein Produkt erworben hat und dabei entweder dem Versand eines Newsletters zum Produkt (oder anderer benannter Produkte) ausdrücklich zugestimmt hat, oder dass der Unternehmer i.R.d. Erlangung der E-Mail-Adresse auf den Versand des Newsletters und der Möglichkeit des Widerspruchs ohne zusätzliche Übermittlungskosten hingewiesen hat. Im ersten Fall richtet sich die Zulässigkeit der Newsletter-Übersendung nach § 7 Abs. 2 Nr. 3 UWG, Art. 6 Abs. 1 lit. a DS-GVO, während im zweiten Fall sich die Rechtgrundlage in § 7 Abs. 3 UWG, Art. 6 Abs. 1 lit. f DS-GVO findet.

Hier sind die häufigsten Fehler im Fall des § 7 Abs. 3 UWG zu finden, indem die Voraussetzungen der Ziffern 1 bis 4 zumeist nicht kumulativ vorliegen, sondern meist der Hinweis nach Ziffer 4 fehlt oder dieser nicht nachweisbar ist. Selbst wenn alle Voraussetzungen gegeben sind, verhindert § 7 Abs. 3 Nr. 2 UWG die Nutzung für die Bewerbung von Konzernunternehmen oder deren Produkten.

Auch im Fall der ausdrücklichen Einwilligung in den Versand eines Newsletters zu dem konkreten oder ähnlichen Produkt ist in aller Regel das konzernweite Cross-Marketing ausgeschlossen. Bei der Auslegung der Einwilligung des Kunden sind nämlich nicht nur die allgemeinen Auslegungsregeln nach §§ 133, 157 BGB zu beachten, sondern natürlich auch der Grundsatz der Zweckbindung im Datenschutzrecht.

Das Prinzip der Zweckgebundenheit der Einwilligung folgt aus dem Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b DS-GVO. Dieser besagt, dass personenbezogene Daten nur für – zuvor! – festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Das bedeutet, dass sie nicht in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden dürfen. Der Zweck gibt an, warum bestimmte personenbezogene Daten erhoben und verarbeitet werden. Bei der Zweckbindung laut DS-GVO sind folgende Dinge zu beachten:

- Vor der Erhebung und Verarbeitung muss der Zweck festgelegt werden.
- Der Zweck muss eindeutig sein und ein gesetzlicher Erlaubnistatbestand (vgl. Art. 6 DS-GVO) vorliegen.
- Bei einer Zweckänderung, wenn die personenbezogenen Daten also anderweitig verarbeitet werden, bedarf es eines neuen Erlaubnistatbestands gem. Art. 6 DS-GVO.

Soweit der Kunde also lediglich in den Versand eines Newsletters durch ein konkretes Unternehmen für ein konkretes oder ähnliches Produkt zugestimmt hat, so ist eine nachträgliche Erweiterung dieser Einwilligung auf Konzernunternehmen nicht möglich. Dabei sind auch hinsichtlich der Frage, für welche anderen Produkte eine Werbung erfolgen darf, erhöhte Anforderungen an die Transparenz zu stellen. Hier muss es die Einwilli-

gungserklärung (also Produkte oder Produktgruppen) klar benennen, damit der Kunde auch die Reichweite seiner Einwilligung erfassen kann und eine Abgrenzung möglich ist. Der *BGH* hatte zuletzt dabei auf die Anforderungen der §§ 305 ff. BGB aus dem Recht der Allgemeinen Geschäftsbedingungen zurückgegriffen,[1] insbesondere das Transparenzgebot, da eben auch die Einwilligungserklärung üblicherweise durch das werbende Unternehmen vorformuliert wird.

Nicht nur die Einwilligung selbst kann zu einer Eingrenzung der zulässigen Werbung führen, auch aus anderen Gesetzen können sich hier Einschränkungen ergeben. In der Games-Branche ist hier spezifisch der Jugendmedienschutzstaatsvertrag zu nennen. Werbung für Angebote, die geeignet sind, Kinder und Jugendliche in ihrer Entwicklung zu beeinflussen oder deren Interessen zu schaden, müssen getrennt von anderer Werbung gesendet werden (§ 6 Abs. 3 und Abs. 4 JMStV),[2] insbesondere dann, wenn bekannt ist, dass der Empfänger kein Erwachsener ist. Auch ist darauf hinzuweisen, dass in beiden Fällen dem Kunden die Möglichkeit gegeben werden muss, jederzeit vom weiteren Bezug des Newsletters Abstand zu nehmen. Für die erste Fallgruppe folgt dies schon aus dem Wortlaut des § 7 Abs. 3 Nr. 4 UWG und Art. 21 Abs. 1 DS-GVO, während für die zweite Fallgruppe sich die Widerruflichkeit aus der Natur der Einwilligung im UWG als widerrufliche Erklärung[3] ergibt sowie aus Art. 7 Abs. 3 DS-GVO. In beiden Fällen bleibt der Versand bis zum Eingang des Widerrufs zulässig, da ein Widerruf nur für die Zukunft Wirkung entfaltet.[4]

Selbst wenn dies nicht gesetzlich vorgeschrieben ist, empfiehlt es sich, als Nachweis für eine Einwilligung bzw. den rechtmäßigen Kaufabschluss das sog. „Double-Opt-in-Verfahren" zur Validierung der E-Mail-Adresse durchzuführen.[5] Werden gleichzeitig mehrere Erklärungen abgegeben, z.B. Anmeldung eines Kundenkontos und Anmeldung für einen oder mehrere Newsletter, so genügt die Übersendung einer einzelnen Bestätigungs-E-Mail für das Double-Opt-in. Da die Double-Opt-in-E-Mail lediglich der Verifizierung der Zugriffsberechtigung auf das angegebene E-Mail-Konto dient und nicht etwa die rechtsverbindliche Erklärung wiederholt, liegt auch keine möglicherweise unzulässige Verbindung mehrerer Erklärungen vor. Schließlich ist der Versand nur einer Bestätigungs-Mail auch im Interesse des Kunden, der nicht jedes Mal erneut seine E-Mail-Adresse verifizieren will, wenn dies bereits einmal geschehen ist.

2. Unternehmens-Newsletter

Ein Unternehmens-Newsletter bezieht sich grundsätzlich auf Informationen zu einem konkreten Unternehmen und dessen Produkten. Insofern ist der inhaltliche Rahmen für einen Unternehmens-Newsletter stets weiter als der enge Rahmen eines Produkt-Newsletters, der immer auf ein konkretes Produkt oder ähnliche Produkte beschränkt ist. Um den Anforderungen der Rechtsprechung an das Transparenzgebot[6] genüge zu tun, dürfte eine Generaleinwilligung wie „für beliebige Produkte" jedoch nicht ausreichend sein.[7] Vielmehr muss der Umfang der Einwilligung zumindest nachvollziehbar umrissen sein, z.B. „und sonstige Printprodukte"[8]. Auch kann sich der Unternehmens-Newsletter auf Informationen zum Unternehmen und dessen Entwicklung ohne Produktbezug beschränken. Insofern kommt als Rechtsgrundlage hier lediglich die Einwilligung nach § 7 Abs. 2 Nr. 3 UWG, Art. 6 Abs. 1 lit. a DS-GVO in Betracht.

3. Konzern-Newsletter

Im Fall eines Konzern-Newsletters kann die Stoßrichtung in zwei verschiedene Richtungen gehen: Zum einen soll entweder allen Unternehmen des Konzerns das Recht zum Newsletter-Versand eingeräumt werden oder einem Unternehmen soll das Recht zum Newsletter-Versand hinsichtlich aller Produkte und Leistungen seines Konzerns eingeräumt werden. In beiden Fällen richtet sich die Wirksamkeit der Einwilligungen nach § 7 Abs. 2 Nr. 3 UWG und Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO.

Ihre Grenze findet eine solche Einwilligung in einen Konzern-Newsletter erneut im Transparenzgebot. Wie der *BGH* mehrfach ausgeführt hat,[9] muss die Einwilligungserklärung nicht nur im Hinblick auf die Produkte, die beworben werden dürfen, transparent gestaltet sein (s. unten) – das Transparenzgebot gilt auch im Hinblick auf die Absender, denen der Versand erlaubt werden soll. Ein unbestimmter Verweis auf nicht näher benannte Konzernunternehmen genügt diesen Anforderungen nicht. Jedoch auch die Nennung einer sehr großen Anzahl an Unternehmen (z.B. 20 Unternehmen) dürfte für den Verbraucher nicht mehr transparent sein. Insofern kann nur angeraten werden, sich auch beim Konzern-Newsletter auf bestimmte Unternehmen und deren Produkte zu konzentrieren. Das *OLG Frankfurt/M.* hat zumindest die Nennung von acht Konzernunternehmen noch für zulässig erachtet.[10] Daneben gilt auch weiterhin, dass i.R.d. Einwilligung hinsichtlich der Produkte und Dienstleistungen eine thematische Einschränkung i.S.d. Transparenzgebots erfolgen muss.

III. Versand durch Dritte

In einem Konzern gibt es regelmäßig eine Abteilung, die für den konzernweiten Newsletter-Versand oder zumindest für ein koordiniertes Marketing zuständig ist. Nicht jedes Gruppen-Unternehmen veranlasst den Newsletter-Versand selbst, dies wäre nicht zweckmäßig. Die folgenden Punkte sollten an die für den konzernweiten Newsletter-Versand zuständige Abteilung klar kommuniziert und auch nachgehalten werden.

Der Versand eines Newsletters für Unternehmen A darf auch durch Unternehmen B versandt werden: Voraussetzung ist, dass der Versand des Newsletters nach den o.g. Kriterien durch Unternehmen A zulässig ist und ein entsprechender Auftragsverarbeitungsvertrag gem. Art. 28 Abs. 3 DS-GVO zwischen Unternehmen A („Verantwortliche Stelle") und Unternehmen B („Auftragsverarbeiter") vorliegt. Einer gesonderten Einwilligung durch den Kunden bedarf es in diesem Fall nicht.

Ein Vertrag über die Verarbeitung der Daten im Auftrag ist auch dann nicht obsolet, wenn der betreffende Kunde eine Newsletter-Einwilligung in den Erhalt von Newslettern von mehreren Gruppen-Unternehmen (einschließlich Unternehmen B) erteilt hat: Eine solche Einwilligung würde zwar Unternehmen B ermächtigen, im eigenen Namen einen Newsletter zu versenden. Soweit dies jedoch im Auftrag von Unternehmen A geschieht, bleibt Unternehmen A verantwortliche Stelle und dem Unternehmen A gegenüber müssen die Einwilligungsvoraussetzungen vorliegen. Dass diese parallel auch für Unternehmen B im eigenen Namen als verantwortliche Stelle vorliegen würde, ändert an diesem Umstand nichts.

Schließlich kann auch das sog. „kleine Konzernprivileg", das in Erwägungsgrund 48 DS-GVO seine Erwähnung findet, eine sol-

1 *BGH* ZD 2017, 327 m. Anm. *Eckhardt*.
2 Beck'scher Komm. zum Rundfunkrecht/*Ladeur*, 4. Aufl. 2018, JMStV § 6 Rn. 24-25.
3 Fezer/Büscher/Obergfell/*Mankowski*, UWG, Komm., 3. Aufl. 2016, § 7 Rn. 151, 152
4 *Gola*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 54-58
5 Spindler/Schuster/*Micklitz*/*Schirmbacher*, Recht der elektronischen Medien, 4. Aufl. 2019, UWG § 7 Rn. 130-137, mit umfangreichen wN.
6 *BGH* ZD 2017, 327 m. Anm. *Eckhardt*.
7 *Mankowski* (o. Fußn. 3), Rn. 137a.
8 *Koreng*/*Lachenmann*, Formularhdb. Datenschutzrecht, 2018, 2. Rn. 5.
9 *BGH* MMR 2013, 380 m. Anm. *Eckhardt*; *BGH* ZD 2017, 327 m. Anm. *Eckhardt*.
10 *OLG Frankfurt/M.* ZD 2019, 507 m. Anm. *Eckhardt*.

che Auftragsverarbeitungsvereinbarung nicht ersetzen: Nach Erwägungsgrund 48 ist es denkbar, dass verbundene Unternehmen personenbezogene Daten für rein interne Verwaltungszwecke auf der Grundlage berechtigter Interessen nach Art. 6 Abs. 1 lit. f DS-GVO an andere verbundene Unternehmen als verantwortliche Stelle übermitteln.[11] Klassische Beispiele hierfür sind eine einheitliche Personalabteilung oder Buchhaltung.[12] Vorliegend geht es jedoch nicht um interne Verwaltungsmaßnahmen, sondern um offenkundige externe Produktwerbung. Die Anwendung des kleinen Konzernprivilegs würde hier die Zweckbindung der Einwilligung über Gebühr ausdehnen.

Es ist in diesen Fällen auch das Transparenzgebot gem. § 6 Abs. 1 TMG zu beachten, das ausdrücklich in § 7 Abs. 2 Nr. 4b UWG referenziert ist: Danach muss aus dem Newsletter leicht erkennbar, unmittelbar erreichbar und ständig verfügbar die Identität des verantwortlichen Absenders (nicht des Dienstleisters) hervorgehen.[13] Die Nennung des Dienstleisters ist nicht verboten, soweit der verantwortliche Absender klar erkennbar bleibt, umsetzbar z.B. durch Versand durch Konzern-Unternehmen B im Auftrag von Konzern-Unternehmen A. Dabei genügt grundsätzlich auch ein Link auf eine Webseite mit den Impressumsangaben, nicht ausreichend ist die Wiedergabe eines Firmenlogos.[14]

Zwischenfazit

Ein sog. „Konzernprivileg" bei der konzernweiten Nutzung von Adress- und anderen Kundendaten zum Zwecke des Newsletter-Versands besteht nicht. Das „kleine Konzernprivileg" ist argumentativ vertretbar, rechtfertigt in der Folge aber auch keinen Zugriff auf Adressdaten eines anderen Konzernunternehmens für eigene Zwecke, da das kleine Konzernprivileg nur für sog. „interne Verwaltungszwecke" gelten kann. Der Newsletter-Versand aber weder eine „interne" Angelegenheit ist noch Verwaltungszweck, sondern als Werbung einschlägig ist.

IV. Hinzukommende Unternehmen zum Konzernverband

Wird ein Unternehmen vom Konzernverbund durch Übernahme von Gesellschaftsanteilen hinzugekauft, sind auch bei einem bestehenden Konzern-Newsletter verschiedene Dinge zu beachten. Grundsätzlich ist der Unternehmenskauf in Form der Übernahme der Gesellschaftsanteile bzw. der Verschmelzung eine datenschutzrechtlich recht unbedenkliche Variante (im Vergleich zu z.B. Asset-Kauf), da der Rechtsträger erhalten bleibt – und damit auch etwaige zuvor zu dessen Gunsten eingeholte Einwilligungen bestehen bleiben.

Hier sollte natürlich vom erwerbenden Unternehmen – möglichst schon i.R.e. zuvor stattgefundenen Due Diligence – die rechtskonforme Einholung der Einwilligungen bzw. das Vorliegen der Voraussetzungen nach § 7 Abs. 3 UWG und deren lückenlose Dokumentation geprüft worden sein. Ein Newsletter-Datenbestand ist praktisch nur risikolos nutzbar, soweit die rechtlichen Voraussetzungen nachweisbar dokumentiert sind, um im Falle eines behaupteten Verstoßes den Beweis der Einwilligung zu führen, insbesondere durch die Dokumentation des Double-Opt-in-Verfahrens.[15]

Aber selbst, wenn die Prüfung keinerlei rechtliche Auffälligkeiten gezeigt hat, steht der Konzern nun vor dem Problem, dass die im Wege des Unternehmenskaufs eingekauften Einwilligungen sich nur auf den Erhalt eines Newsletters von dem erworbenen Unternehmen beziehen. Hier ergibt sich folgende Hürde: Die „Alt-Unternehmen" im Konzern können den „Neuling" nicht einfach in ihre Newsletter-Kommunikation mit aufnehmen – und das neu akquirierte Unternehmen kann nicht einfach Produktwerbung der Alt-Unternehmen in seinen Newsletter integrieren. Dieses Hindernis gilt natürlich nur für Bestandskunden – es ist insofern zu empfehlen, bei Akquisition eines Unternehmens auch zeitnah die Einwilligungstexte hinsichtlich des Newsletter-Versands anzupassen und zu erweitern; auf Seiten des neuen Unternehmens, aber natürlich auch bei den bereits vor Akquise im Konzern vorhandenen Gruppen-Unternehmen.

Aus der Praxis heraus hat sich dabei die Incentivierung der Kund*innen für eine erweiterte Newsletter-Einwilligung – z.B. durch Teilnahme an einem Gewinnspiel oder bei Games das Angebot besonderer Items/Spielgegenstände – als besonders effektiv erwiesen. Solche Anreizsysteme sind auch nicht durch ein eventuelles Kopplungsverbot untersagt, solange die dem Verbraucher angezeigten Erklärungsinhalte dem Transparenzgebot entsprechen,[16] wobei das *OLG Frankfurt/M.* zuletzt eine Einwilligung für wirksam gehalten hat, obwohl die Geschäftsbereiche der Konzernunternehmen nicht weiter definiert waren.[17] Vielmehr führte das *OLG Frankfurt/M.* aus, dass dann die Einwilligung dahingehend zu verstehen sei, dass sich diese nur auf die ausdrücklichen Geschäftsbereiche des Hauptunternehmens bezieht und dies nicht zur Unwirksamkeit an sich führt.

V. Einsatz externer Dienstleister beim Versand

1. Mandantenfähigkeit beachten

Eher die (goldene) Regel als die Ausnahme ist der Einsatz eines externen Dienstleisters, der den Newsletter-Versand für die Konzernunternehmen organisiert und durchführt. Diese Anbieter sind spezialisiert auf den Versand und das Tracking von Newsletter-Aussendungen. Dabei werden üblicherweise die Empfängerdatenbanken auf einem Computersystem des Dienstleisters geführt und der Dienstleister organisiert regelmäßig auch die Durchführung des Double-Opt-in bei der Newsletter-Anmeldung.

Eine direkte Verbindung zwischen den Kundendatenbanken des Unternehmens und der Datenbank des Dienstleisters besteht in aller Regel nicht, es sind also autarke Datenbanken, was auch schon durch das Trennungsgebot nötig ist.[18]

In dieser Konstellation ist der Abschluss einer Auftragsverarbeitungsvereinbarung zwischen der verantwortlichen Stelle und dem Dienstleister gem. § 28 Abs. 3 DS-GVO geboten. Dabei ist gerade beim Konzern-Newsletter darauf zu achten, dass die verantwortliche Stelle hier immer der jeweilige Versender des Newsletters ist und entsprechend alle (!) i.R.d. Einwilligung einbezogenen Konzernunternehmen eine Auftragsverarbeitungsvereinbarung abschließen müssen. Dies ist theoretisch auch für alle Unternehmen in einem Dokument vorstellbar, soweit dabei darauf geachtet wird, dass die Vertretungsverhältnisse gewahrt werden. Vor dem Hintergrund der rechtlichen Selbstständigkeit der Unternehmen empfiehlt es sich jedoch, jeweils einzelne Verträge abzuschließen, auch wenn diese ggf. zentral bezahlt werden.

11 *Nickel*, ZD 2021, 140 (143).
12 *Laue*, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 1 Rn. 46.
13 *Sesing*, in: BeckOK IT-Recht, Stand: 1.9.2020, TMG § 6 Rn. 23-25.
14 Spindler/Schmitz/*Spindler*, TMG, 2. Aufl. 2018, § 6 Rn. 21, 22.
15 Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht, 3. Aufl. 2019, Rn. 129-136.
16 *Gola* (o. Fußn. 4), Rn. 31.
17 *OLG Frankfurt/M.* ZD 2019, 507 m. Anm. *Eckhardt*.
18 *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil XII. Kap. 2 E.VIII. Rn. 92.

Es sollte vor der Wahl eines externen Dienstleisters genau geprüft werden, ob der Anbieter in der Lage ist, nach den Vorgaben des aus der DS-GVO folgenden Trennungsgebots die Daten des Endkunden – also mindestens dessen E-Mail-Adresse, aber auch die Dokumentation und den materiellen Umfang der vom Kunden erteilten Einwilligung – getrennt von den Daten des Kunden anderer Konzern-Unternehmen, zu organisieren. Die sog. Mandantenfähigkeit soll in erster Linie vermeiden, dass Daten, die zu einem vorher festgelegten Zweck erhoben wurden, mit Daten vermengt werden, die zu einem anderen Zweck erhoben wurden.[19] Damit wird sichergestellt, dass die Zweckbindung auch im Verhältnis zu jedem einzelnen Konzernunternehmen gewahrt bleibt.[20] Es empfiehlt sich grundsätzlich schon aus Compliance-Gründen, die angebotene Auftragsverarbeitungsvereinbarung im Hinblick auf die technischen und organisatorischen Maßnahmen genauer zu prüfen.

2. Dienstleister im Drittstaat: Neue Klauseln, neues Glück?

Soweit der Dienstleister seinen Sitz außerhalb der Europäischen Union hat und kein Angemessenheitsbeschluss nach Art. 45 DS-GVO vorliegt, ist zusätzlich zu prüfen, inwiefern vom Anbieter die Standardklauseln der *EU-Kommission* nach Art. 28 Abs. 6, 7 DS-GVO angeboten werden. Die anderen denkbaren Ausnahmen nach Art. 46 Abs. 2 DS-GVO sind in der Praxis irrelevant. Dabei ist zu beachten, dass die *EU-Kommission* am 4.6.2021 ein neues Set an Standardklauseln veröffentlicht hat, die ab sofort verwendet werden sollten.[21] Altverträge unter Verwendung der alten Standardklauseln dürfen noch während einer Übergangsfrist von 18 Monaten gem. Erwägungsgrund 24 des Durchführungsbeschlusses (EU) 2021/914 verwendet werden. Dabei ist allerdings zu beachten, dass die alleinige Verwendung der alten (wie auch der neuen) Standardklauseln vor dem Hintergrund der Schrems-II-Entscheidung des *EuGH*[22] gerade mit Bezug auf die Vereinigten Staaten heute nicht mehr als ausreichend angesehen werden. Vielmehr verlangt der *EuGH* in der Schrems-II-Entscheidung, dass die Standardklauseln durch angemessene Regelungen zu ergänzen sind, die die Risiken eines Übergriffs durch Behörden des Drittlands für den Betroffenen kompensieren.[23] Es obliegt insofern nunmehr jedem Unternehmen selbst, zu prüfen, ob und wenn ja, welche ergänzenden Garantien im Zielstaat notwendig oder ausreichend sind. Da es keinerlei Vorgaben hierzu gibt, liegt das Risiko derzeit allein beim datenexportierenden Unternehmen. *Microsoft*, *Google* und andere Anbieter bieten zwischenzeitlich schon solche zusätzlichen Garantien an, ob diese jedoch nach den Maßstäben des *EuGH* ausreichend sind, ist fraglich. Der *Europäische Datenschutz Ausschuss (EDSA)* selbst geht davon aus, dass eine Kompensation der Risiken staatlicher Eingriffe vertraglich nicht möglich ist.[24] In diesem Fall hätte der *EuGH* alle Verwender wohl in eine veritable Falle gelockt mit seinen Anforderungen. Aus Praxissicht bleibt die Empfehlung, darauf zu achten, dass zusätzliche Garantien – ggf. auch technischer Natur – angeboten werden, da ansonsten zumindest im Fall der USA nicht von einem zulässigen Datenexport ausgegangen werden kann.

19 *Jandt/Steidle*, Datenschutz im Internet, 1. Aufl. 2018, A.II.1.d)bb) Rn. 42.
20 *DSK*, Orientierungshilfe Mandantenfähigkeit.
21 Vgl. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de.
22 *EuGH* MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel* – Schrems II.
23 *Schwartmann/Burkhardt*, ZD 2021, 235; *Heinzke*, GRUR-Prax 2020, 436.
24 *EDSA*, Empfehlungen 01/2020, Rn. 48.

VI. Austragen bitte – aber wovon konkret?

Auch wenn dies auf den ersten Blick unverständlich klingen mag, kann die effektive Umsetzung von Löschungsersuchen gerade bei einer konzernweiten Newsletter-Lösung durchaus kompliziert sein. Dabei beginnt die Problematik bereits mit der Frage, was als Löschungsersuchen für ein Newsletter-Abonnement anzusehen ist und endet damit, wie Daten gleichzeitig und auch rechtzeitig aus einer Vielzahl grundsätzlich voneinander unabhängiger Datenbanken entfernt werden können.

1. Account-Kündigung

Games-Publisher und Vertriebsplattformen bieten den Kund*innen üblicherweise an, ein Kundenkonto („Account") anzulegen. Dieser Account dient häufig sowohl als Kundenkonto für Einkäufe oder für Social-Media-Angebote wie Foren, als auch als Authentifizierung für den Download gekaufter Spiele oder die Anmeldung für eines oder mehrere Online-Spiele. Häufig wird ein allgemeines Kundenkonto („Plattform-Account") angelegt, das dann weitere Unterkonten („Spiele-Accounts") enthält. Rechtlich handelt es sich hierbei um getrennte Vertragsbeziehungen. Ein Vertragsverhältnis für die Nutzung der Plattform und ein eigenes Vertragsverhältnis für die Nutzung des konkreten Spiels.

Tatsächlich ist es sogar häufig so, dass bei Games-Unternehmensgruppen der Plattformbetrieb bei einem der Konzernunternehmen zentriert wird, während die unterschiedlichen Unternehmen der Unternehmensgruppe dort im eigenen Namen und auf eigene Rechnung ihre Leistungen anbieten. Demnach ist es gut möglich, dass der Plattform-Account mit Unternehmen A abgeschlossen wird, der Spiele-Account aber mit Unternehmen B und/oder Unternehmen C.

Kündigt also ein Kunde „seinen Account" stellt sich die Frage, ob davon auch die Abbestellung eines Newsletters umfasst ist. Hierbei ist grundsätzlich die Erklärung des Kunden nach §§ 133, 157 BGB auszulegen.

a) Spiele-Account

Kündigt der Kunde einen Spiele-Account, dürfte es im Zweifel unstreitig sein, dass ein durch den Kunden zuvor bestellter Unternehmens- oder Konzern-Newsletter hiervon nicht umfasst ist. Mit der Kündigung eines konkreten Spiels gibt der Kunde nicht ohne Weiteres zu erkennen, dass er nicht mehr an Informationen zum Unternehmen oder zum Konzern interessiert ist.

Jedoch auch im Hinblick auf den Produkt-Newsletter geht allein aus der Kündigung eines Spiele-Accounts nicht zweifelsfrei hervor, dass der Kunde nicht mehr an dem Produkt oder ähnlichen Produkten interessiert ist. So ist es nicht ausgeschlossen, dass der Kunde lediglich eine Pause beim Spielen einlegen will, dabei aber weiter informiert sein will für den Fall, dass er wieder mit dem Spielen beginnen möchte. Gerade bei der Kündigung eines Abonnements, das später wieder aufgenommen werden kann, ist ein solcher Löschungswille nicht erkennbar. Zumindest vorstellbar ist es, dass ein Kunde, der einen Spiele-Account kündigt und dabei auch die Löschung seiner Spieldaten verlangt, kein Interesse mehr an einem reinen Produkt-Newsletter hat.

Einige Datenschutzbehörden sehen das Löschbegehren als klaren Hinweis darauf, dass der Kunde auch aus dem Produkt-Newsletter ausgetragen werden möchte. Das ist insoweit absolut verständlich, wenn die Kündigung mit einem allgemeinen Löschungsersuchen einhergeht. Kündigt der Kunde dagegen nur einen von mehreren Spiele-Accounts bei Unternehmen B oder wird lediglich ein Abonnement gekündigt, das jederzeit wieder aufgenommen werden kann, so spricht nichts dafür, dass der Kunde kein Interesse mehr an entsprechenden Produktinformationen hat.

b) Unternehmens-Account

Kündigt der Kunde seinen Account pauschal für alle Angebote eines Unternehmens oder für die gesamte Plattform – also eine Kündigung, die ggf. auch mehrere Spiele-Accounts umfasst – so ist die Auslegung durchaus schwieriger, da er zu erkennen gibt, dass er kein Interesse am Angebot hat. Wenn allerdings ein Spiel später durch neuen Abschluss eines Accounts fortgesetzt werden kann, ist es eben nicht eindeutig, ob wirklich kein grundsätzliches Interesse mehr besteht oder ob nur temporär kein Nutzungsinteresse, das Informationsinteresse aber noch gegeben ist.

Während die sicherste Lösung die Löschung aus dem Unternehmens-Newsletter ist, entspricht dies nicht den Interessen des Unternehmens und mutmaßlich auch nicht zwingend den Interessen des Kunden. Es hat sich daher in der Praxis als durchaus praktikabel erwiesen, einem kündigenden Kunden vor Abschluss einer Kündigung (oder soweit diese per E-Mail erfolgte: i.R.d. Eingangsbestätigung) darauf hinzuweisen, dass er seine Newsletter-Abonnements selbstständig verwalten kann und ihn auf eine Webseite weiterzuleiten, bei der er sich manuell aus den ggf. abonnierten Newslettern austragen kann; dies kann in der Form bekannter Consent-Manager-Systeme (CSM) erfolgen.[25] Vor dem Hintergrund der Vielzahl von auslegungsbedürften Willenserklärungen – häufig haben Games-Unternehmensgruppen mehr laufende Accounts in zwei- bis dreistelliger Millionenzahl – dürfte eine solche Lösung für alle Parteien interessensgerecht sein, soweit eine schriftliche Kündigung im Einzelfall nicht absolut eindeutig war. Auch entspricht eine solche technische Lösung der Anforderung des „Privacy by Design" i.S.d. Art. 25 DS-GVO.

Diese Lösung ermöglicht auch, das größte technische Problem in diesen Kündigungsfällen in den Griff zu bekommen. Wie bereits dargestellt, sind die Newsletter-Datenbanken üblicherweise ausgelagert an externe Diensteanbieter, zumindest aber an eine zentrale Stelle im Unternehmensverbund. Diese Newsletter-Datenbanken sind meist nicht mit den Account-Datenbanken der Unternehmen verbunden. Eine Löschung eines Accounts oder der Accountdaten hat daher im Regelfall keinerlei Auswirkung auf die Newsletter-Datenbanken. Tatsächlich geht meist aus der Account-Datenbank nicht einmal hervor, ob der Kunde jemals überhaupt einen Newsletter bestellt hat oder nicht.

Soweit also auch eine Newsletter-Abmeldung intendiert ist, muss sichergestellt werden, dass eine Löschung auch in der getrennten Datenbank erfolgt. Noch komplexer wird es, wenn für mehrere Produkte – und dann auch noch für eine Mehrzahl von Unternehmen – gesonderte Newsletter-Datenbanken bestehen. Dies kann natürlich manuell sichergestellt werden, in dem ein Kundendienst händisch Datenbanken abgleicht, dies dürfte aber kaum praktisch umsetzbar sein. Daher bietet sich ein o.g. CSM an. Dies ist jedoch nur realistisch umsetzbar, soweit auch die jeweiligen Newsletter-Diensteanbieter Schnittstellen zur Verfügung stellen, die ein solches Management ermöglichen. Hier empfiehlt es sich tunlichst, diese Voraussetzungen schon i.R.d. Beschaffung anzusprechen und sodann konzeptionell mit dem Anbieter umzusetzen.

2. Newsletter-Abmeldung

Nutzt der Kunde einen Link oder einen Button zum Abmelden von einem Newsletter (z.B. im Footer eines Newsletters), so ist davon auszugehen, dass der Kunde nur den konkreten Newsletter abbestellen will. Eine Pflicht, den Kunden auf einen entsprechenden Consent-Manager auch für andere Newsletter zu leiten oder ihm dies zumindest anzubieten, besteht nicht. Ein Unternehmen muss dem Kunden Abmeldemöglichkeiten nicht aufdrängen, sondern nur dort zur Verfügung stellen, wo gesetzlich gefordert.

3. Datenlöschungsersuchen

Ebenfalls eindeutig ist die Behandlung im Rahmen eines Datenlöschungsersuchens. Wünscht ein Kunde die Löschung aller löschungsfähigen Daten (soweit also kein Hinderungsgrund nach Art. 17 Abs. 3 DS-GVO vorliegt), umfasst dies ebenfalls etwaige Newsletter-Abonnements. Da mit dem Löschungsersuchen gleichzeitig der Widerruf der Einwilligung in den Empfang des Newsletters sowohl nach UWG als auch nach DS-GVO zu erkennen ist, muss der Anbieter auch sicherstellen, dass ein weiterer Newsletter-Versand ab Zugang nicht mehr erfolgt. Die Wirkung des Widerrufs tritt sofort ein,[26] sodass auch die Wirksamkeit einer z.B. in den AGB vereinbarten „Umsetzungsfrist" zumindest fraglich sein dürfte. Ein Konzept, das auf einer manuellen Umsetzung solcher Löschungsersuchen basiert, dürfte daher grundsätzlich problematisch sein, da die Wirkung der fehlenden Einwilligung sofort eintritt, während bei der Löschungspflicht zumindest eine Löschung ohne schuldhaftes Zögern nach Art. 17 Abs. 1 DS-GVO besteht,[27] was nach Art. 12 Abs. 3 DS-GVO auf höchstens einen Monat beschränkt ist. Um eine automatisierte Lösung wird man daher kaum herumkommen. Ist die Erklärung jedoch nicht eindeutig, so ist dem Erklärungsempfänger zumindest eine Rückfrage einzuräumen, z.B. über den o.g. Consent-Manager.

Eine solche Lösung sollte i.R.d. Datenlöschungskonzepts geplant und unternehmensweit umgesetzt werden, um den Versand und die Abmeldung von Newslettern sicher und praktikabel zu gestalten.

Schnell gelesen ...

- Der Newsletter-Versand sollte – auch und gerade im Konzern – intern aber auch extern (Dienstleister) aus einer Hand organisiert und nachgehalten werden.
- Externe Dienstleister beim Newsletter-Versand sind vor Vertragsschluss insbesondere mit Blick auf ihre Mandantenfähigkeit aber auch auf ihren Sitz zu prüfen.
- Auch im Falle umfassender Einwilligung des Kunden in einen Konzern-Newsletter sind regelmäßig konzern-interne Auftragsverarbeitungsverträge abzuschließen.
- Technische Lösungen müssen die erheblichen Anforderungen der Abwicklung von großen Kundenbeständen, aber auch der vielen verschiedenen Datenbanken i.S.d. „Privacy by Design" berücksichtigen.

Kai Bodensiek
ist Rechtsanwalt und Partner der Brehm & v. Moers Rechtsanwälte Partnerschaftsgesellschaft mbB in Berlin.

David Julian Hoffmann
ist Head of AdTech Legal and Group Data Protection bei der gamigo AG in Hamburg.

25 *Schröder*, Datenschutzrecht für die Praxis, 4. Aufl. 2021, S. 154 ff.
26 *Ehmann/Selmayr*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Rn. 92; *Mankowski* (o. Fußn. 3), Rn. 152.
27 *Ehmann/Selmayr* (o. Fußn. 26), Rn. 40.

ANDREAS LOBER / SUSANNE KLEIN

Datenschutz bei Multiplayer-Games und Spielen auf sozialen Netzwerken

Internationale Datenübermittlung

Spezielle Spiele – spezifische Anforderungen: Globale Datentransfers, halbautomatisierte Entscheidungsfindung und komplexe Verantwortlichkeiten

Die Beliebtheit und der Erfolg von Computerspielen nehmen weiterhin stetig zu. Dies gilt insbesondere für sog. Multiplayer-Games und Spiele auf den großen sozialen Netzwerken. Beiden ist gemein, dass der Spieler regelmäßig nicht allein bleibt, sondern das Spielerlebnis entweder mit anderen teilt oder in den direkten Wettbewerb mit anderen Spieler*innen treten kann. Darüber hinaus bieten Spiele auf sozialen Netzwerken den Vorteil, dass selbst dann, wenn nicht mit „Freunden" aus dem Netzwerk gespielt wird, die Anmeldung zum Spiel besonders einfach ist, weil regelmäßig der bestehende Nutzer-Account hierfür genutzt werden kann. In all diesen Konstellationen werden umfangreiche personenbezogene Daten verarbeitet. Die damit verbundenen datenschutzrechtlichen Fragestellungen betreffen die einschlägigen Rechtsgrundlagen, Verantwortlichkeiten, Betroffenenrechte und nicht zuletzt auch den internationalen Datentransfer, weil für Spieler*innen häufig gerade das globale Spielerlebnis besonders reizvoll ist. Der vorliegende Beitrag konzentriert sich auf die Besonderheiten aus datenschutzrechtlicher Sicht. Lesedauer: 22 Minuten

I. Einleitung

Unter „Multiplayer-Spielen" verstehen wir Spiele, die von einer großen Anzahl von Spieler*innen gleichzeitig mit- oder gegeneinander gespielt werden können, wobei meist Spieler*innen aus aller Welt zeitgleich und in denselben Sessions bzw. Spielewelten teilnehmen können. Darunter fallen Spiele unterschiedlicher Genres, z.B. „Battle Royale"-Spiele (wie „Fortnite" oder „PUBG"), aber auch Online-Rollenspiele[1] wie z.B. „World of Warcraft" oder „Elder Scrolls Online". Diese Spiele leben von einer gewissen Fairness innerhalb des Spiels, weshalb deren Anbieter Maßnahmen treffen, um gegen unfaires Spielen vorzugehen (sog. Anti-Cheating). Dies geschieht in der Regel teilautomatisiert und wirft daher insbesondere Fragen der automatisierten Entscheidungsfindung auf (Art. 22 DS-GVO). Da die Spiele grundsätzlich einem weltweiten Publikum offenstehen, ist meist eine Übertragung von personenbezogenen Daten in Länder außerhalb der Europäischen Union unumgänglich, um den Dienst anbieten zu können. Daher ist die Frage des Datentransfers im Lichte des Schrems-II-Urteils des *EuGH*[2] hier besonders relevant.

Unter Spielen auf sozialen Netzwerken verstehen wir Spiele, die auf den großen Plattformen für die dort registrierten Nutzer*innen angeboten werden, insbesondere „Facebook Instant Games" und „Snap Games".[3] Regelmäßig muss sich der auf dem sozialen Netzwerk angemeldete Spieler dafür kein eigenes Nutzerkonto (Account) beim Spieleanbieter anlegen, sondern kann den Account des sozialen Netzwerks nutzen. Viele dieser Spiele haben die Funktion „Freunde einladen", sodass vor allem mit den vorhandenen „Freunden" auf der jeweiligen Plattform sehr einfach gemeinsame Spiele-Sessions stattfinden können. Aus datenschutzrechtlicher Sicht ist hier besonders die enge Verzahnung mit den sozialen Netzwerken zu beleuchten. Die ersten Spiele auf sozialen Netzwerken waren sog. „Social Games", die meist auch unter die Definition von Multiplayer-Spielen (s.o.) fielen (z.B. „FarmVille")[4]; dies ist aber beileibe nicht bei allen Spielen auf sozialen Medien der Fall. Gerade die aktuell populären Facebook Instant Games sind in der Regel keine Multiplayer-Spiele. Sie leben eher davon, dass Spielerfahrung und -erfolg mit den „Freunden" im sozialen Netzwerk geteilt werden.

II. Multiplayer-Spiele

1. Anti-Cheat

Bei der wohl überwiegenden Anzahl von Multiplayer-Spielen liegt der Reiz (auch) darin, sich mit anderen Spieler*innen zu messen. Einige dieser Spiele setzen vornehmlich auf direkten Wettstreit (z.B. Battle-Royale-Spiele oder Shooter). Doch auch da, wo der Wettstreit gegenüber dem Miteinander weniger stark ausgeprägt ist, spielt Fairness eine wichtige Rolle: Wertvolle Gegenstände beispielsweise wollen erspielt, nicht „ermogelt" sein. Daher gehen viele Anbieter gegen unfaires Spielen vor.[5] Im Zentrum dessen steht das Aufspüren von Drittsoftware, die Nutzer*innen im Spiel nicht vorgesehene Vorteile gibt bzw. Spielfunktionen automatisiert (sog. Cheats, Cheat Bots oder Hacks – nachfolgend: Cheat-Software). Die Anbieter dieser Software agieren oft im Schutz der Anonymität. Derartige Software wurde in zahlreichen Gerichtsentscheidungen als Verstoß gegen Urheber- und Wettbewerbsrecht angesehen,[6] doch ist dies nicht Gegenstand des vorliegenden Beitrags. Vorliegend interessiert nur der datenschutzrechtliche Aspekt. Die meisten Multiplayer-Spiele setzen verschiedene Systeme ein, um Cheat-Software zu erkennen. Dabei handelt es sich teilweise um proprietäre Systeme des jeweiligen Spieleanbieters, teilweise um Softwarelösungen von Drittanbietern (wie BattlEye[7] oder Easy Anti Cheat[8]), oft auch um eine Kombination daraus (nachfolgend: Anti-Cheat-Technologie). Diese Lösungen haben gemein, dass sie verschiedene auf den Spieler bezogene Daten analysieren, um erkennen zu können, ob Cheat-Software eingesetzt wird. Da betrügende Spieler*innen in der Regel vom Spieleanbieter dauerhaft ausge-

1 Englisch als MMORPG abgekürzt, für Massively Multiplayer Online Role Playing Game.
2 *EuGH* MMR 2020, 597 m. Anm. *Hoeren* = ZD 2020, 511 m. Anm. *Moos/Rothkegel* – Schrems II.
3 Die Bedeutung von MySpace und StudiVZ, die beide ebenfalls Social Games anbieten, hat in den vergangenen Jahren deutlich nachgelassen, sodass auf diese Netzwerke im Folgenden nicht vertieft eingegangen wird.
4 Vgl. auch https://www.businessinsider.de/gruenderszene/lexikon/begriffe/social-games/.
5 Für einen kurzen rechtlichen Überblick in englischer Sprache s. z.B. *Lober*, Cheat software: Can publishers level the playing field?, abrufbar unter: https://www.gamesindustry.biz/articles/2020-02-05-cheat-software-in-online-games-how-can-publishers-level-the-playing-field.
6 Vgl. z.B. *BGH* U. v. 6.10.2016 – I ZR 25/15 und *BGH* MMR 2017, 394; vgl. auch *Conraths*, CR 2016, 705 ff.; *Rauda*, MMR-Beilage 8/2019, 20 ff.
7 Vgl. www.battleye.com.
8 Vgl. easy.ac.

schlossen („gebannt") werden, kommt eine anonymisierte Verarbeitung regelmäßig nicht in Betracht.

a) Rechtsgrundlage

Entsprechend stellt sich zunächst die Frage der Rechtsgrundlage. Eine Einwilligung wäre prinzipiell denkbar (Art. 6 Abs. 1 lit. a DS-GVO), ist aber wegen deren freier Widerruflichkeit nicht tauglich. Teilweise argumentieren Spieleanbieter damit, der Einsatz von Anti-Cheat-Technologie sei zur Vertragserfüllung notwendig (Art. 6 Abs. 1 lit. b DS-GVO). Überzeugender erscheint uns der Rückgriff auf berechtigte Interessen (Art. 6 Abs. 1 lit. f DS-GVO). Freilich ist i.R.d. Notwendigkeit bzw. bei der Interessenabwägung auch zu berücksichtigen, wie die durch Anti-Cheat-Technologie verarbeiteten personenbezogenen Daten geschützt werden, auch unternehmensintern. Auf technisch-organisatorische Maßnahmen und kurze Löschfristen sollte daher ein besonderes Augenmerk gelegt werden.

b) Automatisierte Entscheidungsfindung

Bei erfolgreichen Multiplayer-Spielen ist die Zahl der täglich erkannten Betrugsversuche erheblich. Teilweise werden die ertappten Spieler*innen zunächst nur verwarnt, in der Regel aber direkt vom Spiel ausgeschlossen. Bei großen Titeln geht es dem Vernehmen nach oft um tausende Spieler*innen pro Tag. So sollen alleine bei dem Spiel „Call of Duty: Warzone" nach Angaben des Entwicklers an einem einzigen Tag über 30.000 Spieler*innen wegen Cheatings ausgeschlossen worden sein.[9]

Die Entscheidung wird von der Anti-Cheat-Technologie zumindest vorbereitet. Um nicht unter das grundsätzliche Verbot der automatisierten Entscheidungsfindung nach Art. 22 DS-GVO zu fallen und nicht sogar nach Art. 15 Abs. 1 lit. h DS-GVO die Logik der Anti-Cheat-Technologie offenlegen zu müssen (was deren Effektivität erheblich schmälern würde), sollten Spieleanbieter zumindest die Entscheidung über einen definitiven Ausschluss eines Spielers und die Löschung des entsprechenden Accounts nicht ausschließlich automatisiert treffen (vgl. Erwägungsgrund 71). Eine ausschließlich automatisierte Entscheidung wird aber wohl überwiegend auch dann angenommen, wenn eine Person – ohne eigene Erwägungen anzustellen – die automatisierte Vorgabe lediglich bestätigt oder übernimmt.[10]

Dies bedeutet, dass die von der Anti-Cheat-Technologie vorbereitete Entscheidung zumindest von einer Person kontrolliert werden muss. Dies setzt voraus, dass diese über die nötige Datengrundlage verfügt und die fachliche Qualifikation hat. Außerdem muss sie einen Entscheidungsspielraum haben, also befugt sein, von der automatisiert vorbereiteten Entscheidung ggf. auch abzuweichen. Nicht gefordert ist, dass die überprüfende Person die Einzelheiten der Anti-Cheat-Technologie oder deren Algorithmus kennt.[11]

In der Regel werden Spieler*innen, die nach Ansicht des Spieleanbieters gecheatet haben, zunächst temporär von der Teilnahme am Spiel ausgeschlossen, d.h. sie können zunächst nicht mehr teilnehmen, ihr Account bleibt aber bestehen. Sollte sich der Verdacht nicht erhärten, könnten sie wieder für die Teilnahme am Spiel freigeschaltet werden. Richtigerweise wird es sich hierbei nicht um eine Maßnahme mit rechtlicher Wirkung handeln, sondern um eine rein faktische Einschränkung. Im Bereich des Privatrechts haben nämlich vor allem rechtsgeschäftliche Willenserklärungen eine rechtliche Wirkung.[12] Auch eine erhebliche Beeinträchtigung wird regelmäßig nicht vorliegen, sofern der Spiele-Anbieter den Vorgang auf eine Beschwerde des Spielers hin in angemessener Zeit überprüft. Demnach könnte eine temporäre Sperrung eines Accounts nach diesseits vertretener Ansicht regelmäßig auch vollautomatisiert erfolgen, ohne dass ein Fall des Art. 22 DS-GVO vorliegt. In besonderen Fällen – z.B. bei Turnieren mit hohen Preisgeldern – sollte aber ein automatisierter Entscheidungsvorschlag nochmals von einer Person überprüft werden.

Spätestens vor der Kündigung des Spielenutzungsvertrags und irreversiblen Löschung eines Accounts sollte der betroffene Spieler die Möglichkeit haben, um eine von einer Person durchgeführte Überprüfung des Vorgangs zu bitten, was auch dem Leitgedanken des Art. 22 Abs. 3 DS-GVO entspricht. Die Kündigung des Spielenutzungsvertrags wird eine Maßnahme mit rechtlicher Wirkung sein, die irreversible Löschung eines Accounts jedenfalls in manchen Fällen eine erhebliche Beeinträchtigung des Spielers; insbesondere, wenn der Spieler dadurch erhebliche Spielfortschritte oder „virtuelle Besitztümer" verliert.

c) Auskunftsanspruch

Nicht selten kommt es vor, dass „gebannte" Spieler*innen einen Auskunftsanspruch gem. Art. 15 Abs. 1 DS-GVO geltend machen. In diesem Fall ist der Spieleanbieter verpflichtet, Auskunft darüber zu erteilen, ob personenbezogene Daten von dem Spieler verarbeitet werden und, sollte dies der Fall sein, in welchem Umfang dies geschieht. Zu diesem Zweck sieht das Gesetz einen ganzen Katalog zu erteilender Informationen vor, zu denen u.a. die Verarbeitungszwecke, die Kategorien der verarbeiteten Daten, die Empfänger von Daten, die Speicherdauer und nähere Informationen über die Betroffenenrechte gehören (vgl. Art. 15 Abs. 1 DS-GVO). Besonders relevant für „gebannte" Spieler*innen ist die Regelung in Art. 15 Abs. 1 lit. h DS-GVO, wonach auch über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling zu informieren ist, einschließlich aussagekräftiger Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für den Betroffenen.

Obwohl das Auskunftsrecht eines der wichtigsten Rechte für die betroffenen Personen ist, weil es die Betroffenen erst in die Lage versetzen kann und soll, ihre weiteren Rechte zu erkennen und auszuüben, wird es hier häufig nur zu dem Zweck gebraucht, die Einzelheiten über die eingesetzte Anti-Cheat-Technologie zu erfahren. Es geht somit oft weniger um die Wahrung des Datenschutzes, als vielmehr um die Kenntnis der involvierten Anti-Cheat-Logik, z.B. um diese zukünftig umgehen zu können, oder schlicht darum, Druck auf den Spieleanbieter auszuüben.

Der Spieleanbieter muss den Auskunftsanspruch grundsätzlich fristgemäß erfüllen.[13] Etwas anderes gilt nur bei offenkundig unbegründeten oder exzessiven Anträgen, die zwar insbesondere im Fall häufiger Wiederholung vorliegen können (vgl. Art. 12 Abs. 5 S. 1 DS-GVO); gleichwohl sind die Hürden für diese Ausnahmeregelung hoch. Die Grenzen der Auskunftspflicht des Spieleanbieters werden jedoch dort zu ziehen sein, wo seine Betriebs- und Geschäftsgeheimnisse betroffen sind. Schließlich dient der Auskunftsanspruch aus Art. 15 DS-GVO dazu, den Spieler in die Lage zu versetzen, die Verarbeitung seiner personenbezogenen Daten durch den Verantwortlichen überprüfen zu können, damit er ggf. weitere Betroffenenrechte geltend machen kann (vgl. Erwägungsgrund 63 S. 1). Hierdurch dürfen jedoch die Rechte und Freiheiten anderer Personen, etwa Ge-

9 Abrufbar unter: https://www.eurogamer.net/articles/2021-05-16-500-000-cheaters-have-been-banned-from-call-of-duty-warzone.

10 *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 22 DSGVO, Rn. 26 ff. mN.

11 *Scholz* (o. Fußn. 10), Rn. 27; Gola/*Schulz*, DS-GVO, Art. 22 Rn. 16; *von Lewinski*, in: BeckOK DatenschutzR, 36. Ed., Stand: 1.5.2021, DS-GVO Art. 22 Rn. 24.

12 *von Lewinski* (o. Fußn. 11), BDSG § 6a Rn. 25, *Scholz* (o. Fußn. 10), Rn. 34.

13 Die Frist beträgt regelmäßig einen Monat nach Eingang des Antrags und kann in Ausnahmefällen um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist (vgl. Art. 12 Abs. 3 DS-GVO).

schäftsgeheimnisse oder Rechte des geistigen Eigentums, nicht beeinträchtigt werden (Erwägungsgrund 63 S. 5). Es ist nicht erkennbar, weshalb diese Einschränkung nur zu Gunsten anderer Personen gelten soll, der auskunftspflichtige Verantwortliche in Bezug auf seine eigenen Schutzgüter jedoch nicht geschützt sein soll. Es kann daher nicht Sinn und Zweck des Auskunftsanspruchs sein, den Verantwortlichen zu verpflichten, seine eigenen Geschäftsgeheimnisse offenbaren zu müssen. Freilich darf auch diese Einschränkung nur insoweit gelten, als das Auskunftsrecht des Betroffenen hierdurch nicht leerläuft. Es sind jedoch auch die schutzwürdigen Belange des Spieleanbieters zu berücksichtigen, nämlich sein Spiel und die Gewährleistung eines fairen Mit- oder Gegeneinanders der Spieler*innen zu schützen, wenn der Umfang der Auskunftspflicht in Bezug auf die Preisgabe der involvierten Anti-Cheat-Technologie zu bewerten ist.

2. Internationaler Datentransfer

Multiplayer-Spiele zeichnen sich dadurch aus, dass sie Teilnehmer*innen aus aller Welt offenstehen. Diese spielen mit- und gegeneinander. Entsprechend ist es technisch kaum vorstellbar, wie derartige Dienste ohne einen grenzüberschreitenden Austausch personenbezogener Daten realisiert werden könnten. Auch eine vollständige Anonymisierung scheidet in der Regel aus, da zumindest Nutzerkennungen vorhanden sein müssen, die vom Spieleanbieter wieder einer Person zugeordnet werden können. Eine vollständige Verschlüsselung der ins Ausland übertragenen Spielerdaten wird in der Regel ebenfalls nicht möglich sein, da ja gerade eine Kommunikation zwischen Spieler*innen in verschiedenen Territorien möglich sein soll.

Daher scheint in den meisten Fällen keine der vom *Europäischen Datenschutzausschuss* (*EDSA*) als Reaktion auf das Schrems-II-Urteil vorgeschlagenen technischen Möglichkeiten für einen Datenaustausch in potenziell unsichere Drittstaaten ein gangbarer Weg zu sein.[14] Der *EDSA* stellt insbesondere fest, dass es in bestimmten Situationen keine ausreichenden technischen Möglichkeiten zum Schutz personenbezogener Daten gebe, wenn Cloud-Dienste genutzt werden und der Cloud-Dienste-Anbieter Zugang zu unverschlüsselten Daten benötigt.[15] So wird es sich auch bei vielen Multiplayer-Spielen verhalten.[16]

Es lässt sich auch schwerlich sagen, dass von derartigen Transfers nur eine geringe Zahl an Nutzern*innen betroffen ist, wie es die Datenschutzbehörden für die Anwendung von Art. 49 DS-GVO unter Verweis auf das Erfordernis eines nur gelegentlichen Datentransfers generell fordern.[17]

Allerdings ist diese generelle quantitative Einschränkung richtigerweise gar nicht erforderlich: Sofern der internationale Datentransfer z.B. zur Erfüllung des Vertrags notwendig ist oder auf einer Einwilligung beruht, darf er auch massenhaft erfolgen. Notwendig ist freilich, dass die Einwilligung informiert ist – auch in Bezug auf die spezifischen Risiken eines Datentransfers in nicht-sichere Drittstaaten – bzw. bei der Vertragserfüllung an die Notwendigkeitsprüfung strenge Maßstäbe angelegt werden.

Das ergibt sich bereits aus dem Wortlaut der DS-GVO selbst, scheint aber etwas in Vergessenheit geraten zu sein: Zunächst lautet die Überschrift von Art. 49 DS-GVO „Ausnahmen für bestimmte Fälle", enthält also keine quantitative Einschränkung. Eine quantitative Einschränkung ist vielmehr nur in Art. 49 S. 2 DS-GVO vorhanden, welcher lautet: „Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft ...".

Daraus ergibt sich im Gegenschluss, dass bei den in Unterabsatz 1 genannten Fällen gerade keine quantitative Einschränkung gilt, also insbesondere nicht bei einer entsprechend informierten Einwilligung (lit. a) oder zur Erfüllung eines Vertrags zwischen dem Verantwortlichen und dem Betroffenen bzw. entsprechender vorvertraglicher Maßnahmen (lit. b). Dies wird für eine Verarbeitung auf Basis einer Einwilligung auch durch die Erwägungsgründe bestätigt; dort sind allerdings quantitative Einschränkungen für die Verarbeitung zur Vertragserfüllung vorgesehen (vgl. Erwägungsgründe 111 und 113). Allerdings muss der insoweit klare Wortlaut von Art. 49 DS-GVO, der auch für die Verarbeitung zur Vertragserfüllung keine quantitative Einschränkung enthält, den Erwägungsgründen vorgehen.[18] Die Erwägungsgründe dienen nur als Auslegungshilfe.[19]

Die strenge Position des *EDSA* und der deutschen Datenschutzbehörden ist übrigens umso erstaunlicher, weil sie – was die auf Einwilligung gestützte Verarbeitung angeht – im Widerspruch steht zu den *EDSA*-Leitlinien 2/2018[20], auf die in den *EDSA*-Empfehlungen ausdrücklich Bezug genommen wird.[21]

III. Spiele auf sozialen Netzwerken

1. Verantwortlichkeiten

Die Besonderheit bei den Spielen auf sozialen Netzwerken ist, dass ein Dritter, nämlich der jeweilige Plattformbetreiber, mit den personenbezogenen Daten der Spieler*innen in Berührung kommt und diese – je nach Zweck und Vertragslage – verarbeiten kann. Grundlegende Frage ist daher, wer für welche Datenverarbeitungen der Verantwortliche ist.

Auf den ersten Blick erscheint es naheliegend, dass die Verantwortlichkeit für alle Datenverarbeitungen bei dem Plattformbetreiber (Facebook, Snapchat o.Ä.) liegt. Wenn der Nutzer, also der jeweilige Spieler, beim Anlegen seines Accounts den Datenschutzbestimmungen des sozialen Netzwerks zugestimmt hat, müsste dies für alle weiteren Datenverarbeitungen ebenfalls gelten, also auch für die Datenverarbeitungen im Spiel.

Ganz so einfach ist es aber nicht. Sofern Daten vom sozialen Netzwerk an den Spieleanbieter übertragen und auf dessen eigenen Servern verarbeitet und ausgewertet werden, ist das soziale Netzwerk jedenfalls nicht mehr allein verantwortlich. Nach

14 Vgl. die vom *European Data Protection Board (EDPB)* veröffentlichten „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten" v. 10.11.2020, abrufbar unter: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf; neue Version 2.0 v. 18.6.2021, abrufbar unter: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

15 Vgl. Empfehlungen 01/2020 v. 10.11.2020 (o. Fußn. 14), Rn. 88.

16 Anders ggf., wenn sich die Spiele-Server allesamt in der EU oder Ländern mit einem angemessenen Datenschutzniveau befinden; auf Grund der Latenzzeiten befinden sich allerdings Spiele-Server häufig in den unterschiedlichen Weltregionen.

17 Vgl. die PM der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (*Datenschutzkonferenz*) v. 28.7.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf, die auf die vom *EDPB* am 23.7.2020 veröffentlichten „Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems" verweist und die dortige Rechtsauffassung zur engen Anwendbarkeit von Art. 49 DS-GVO (Ziff. 8 der FAQ) ausdrücklich bestätigt.

18 I.E. ebenso *Schröder*, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 49 Rn. 11a.

19 Simitis/Hornung/Spiecker (o. Fußn. 10), Einleitung Rn. 270.

20 Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 VO 2016/679.

21 Vgl. Empfehlungen 01/2020 v. 10.11.2020 (o. Fußn. 14), Rn. 25.

den Kriterien des *EuGH* für Facebook-Fanpages[22] ist eine gemeinsame Verantwortlichkeit jedenfalls naheliegend. Wie bei den Facebook-Fanpages könnte eine gemeinsame Zweck- und Mittelbestimmung vorliegen, und die Einflussnahme auf die Datenverarbeitung dürfte hier in der Gestaltung des Spiels durch den Publisher liegen. Schließlich hat dieser es in der Hand zu bestimmen, welche Daten innerhalb des Spiels erhoben und verarbeitet werden. Die Einordnung kann jedoch nicht schematisch für alle Spiele erfolgen, sondern muss im Einzelfall beurteilt werden. Je datensparsamer das Spiel ausgestaltet ist, desto weniger wird man von einer gemeinsamen Verantwortung ausgehen.

Die Anbieter der wichtigen sozialen Netzwerke scheinen derzeit generell nicht von einer gemeinsamen Verantwortlichkeit auszugehen. Jedenfalls werden keine Verträge über gemeinsame Verantwortlichkeit bereitgestellt. Vielmehr müssen Spieleanbieter die Bedingungen des sozialen Netzwerks akzeptieren, wozu auch die Richtlinien über die Nutzung der angedockten Spiele-Plattform gehören.[23] Darin finden sich je nach sozialem Netzwerk unterschiedliche Regelungen zur datenschutzrechtlichen Verantwortlichkeit; meist wird davon ausgegangen, dass es sich beim Spieleanbieter und dem sozialen Netzwerk um (unabhängige) Verantwortliche handelt.[24] Wenn der Plattform-Anbieter zugleich das Hosting der Spiele übernimmt, wird regelmäßig auch ein Auftragsverarbeitungsvertrag abgeschlossen.[25] In diesem Rahmen werden dann ggf. auch Standarddatenschutzklauseln vereinbart (zu den Besonderheiten des internationalen Datentransfers sogleich s. unter III. 3.).

2. Datenverarbeitungen und Rechtsgrundlagen

a) Daten aus dem Spiel

Beim Spielen auf sozialen Netzwerken finden umfangreiche Datenverarbeitungen statt.[26] Startet der Nutzer eine neue Spiel-Session, teilt ihm das soziale Netzwerk regelmäßig eine individuelle Kennung (ID) zu, die mit den Account-Daten verknüpft wird. Diese Nutzer-ID wird zusammen mit diversen weiteren Daten an den Spieleanbieter übertragen, der diese benötigt, um für den konkreten Nutzer ein Spielerprofil im ausgewählten Spiel zu erstellen und ihm dadurch das Spielen im sozialen Netzwerk zu ermöglichen. Zu diesen Daten gehören in der Regel der (Account-)Name, die Spracheinstellungen, das Land, in dem der Nutzer spielt, ggf. einige technische Daten (wie etwa das Betriebssystem des Endgeräts), bei Facebook auch das Profilbild und die „Freunde", mit denen der Nutzer auf Facebook verbunden ist und die das ausgewählte Spiel ebenfalls schon gespielt haben. Sobald der Nutzer zu spielen beginnt, werden für das jeweilige Spiel die Spieldauer (laufende und pausierende Sessions) sowie der Spielfortschritt und -erfolg (erreichte Level, Highscores, genutzte Hilfen o.Ä.) erfasst, und manchmal auch die Freunde, mit denen zusammengespielt wird. Diese Daten werden nicht nur vom Spieleanbieter selbst verarbeitet, um das Spiel mit all seinen Funktionen bereitstellen zu können. Auf Grund der Verknüpfung mit der vom Plattformbetreiber vergebenen Nutzer-ID werden diese Daten auch dem auf der Plattform hinterlegten Spielerprofil hinzugespeichert und dadurch mit dem Account des Spielers auf dem sozialen Netzwerk verknüpft. Der Plattformbetreiber erhält dadurch viele Daten seiner Nutzer, die er ohne die Bereitstellung der Spiele nicht hätte.

Während sich der Plattformbetreiber für sämtliche Datenverarbeitungen auf der Plattform von seinen Nutzern bei der Account-Erstellung üblicherweise eine umfassende Einwilligung erteilen lässt, deren Wirksamkeit an dieser Stelle nicht weiter thematisiert werden soll, kann sich der Spieleanbieter auf diese Einwilligung im Zweifel nicht berufen. Diese Einwilligung gegenüber dem sozialen Netzwerk, die häufig nach dem Prinzip „One size fits all" sehr weitgehend ausgestaltet ist, kann im Zweifel nicht auch die Datenverarbeitungen im Spiel durch den konkreten Spieleanbieter abdecken. Schwierig ist es z.B., wenn im Zeitpunkt der Account-Erstellung bestimmte Spiele noch gar nicht entwickelt sind und/oder auf der jeweiligen Plattform angeboten werden. Außerdem fehlt es dann bereits an der notwendigen Informiertheit des Nutzers. Besondere Hinweise auf die Spiele erfolgen üblicherweise i.R.d. Account-Erstellung nicht.

In der Regel wird der Spieleanbieter jedoch eine Einwilligung gar nicht benötigen, zumindest so lange nicht, wie er die Nutzerdaten lediglich zum Zwecke der Bereitstellung und Durchführung des konkreten Spiels verarbeitet. In diesem Fall dient die Datenerhebung und -verarbeitung ausschließlich der Vertragserfüllung und ist daher gem. Art. 6 Abs. 1 lit. b DS-GVO gerechtfertigt. Freilich ist insoweit die enge Zweckbindung dieser Datenverarbeitungen auf Seiten des Spieleanbieters zu beachten.

b) Tracking und Analyse

Wenig überraschend ist, dass die beim Spielen in sozialen Netzwerken anfallenden Daten auch ausgewertet werden. Dies geschieht sowohl beim Spieleanbieter als auch beim Plattformbetreiber, wenn auch zu unterschiedlichen Zwecken.

Der Spieleanbieter wertet regelmäßig bestimmte technische Daten sowie Daten aus dem Spielfortschritt aus, was vor allem der Fehleranalyse und -behebung dient. Hierbei wird der Personenbezug meistens vor der Auswertung entfernt (z.B. durch das Hashen der Nutzer-ID), weil es für den verfolgten Zweck nicht auf den konkreten Spieler ankommt. Darüber hinaus erhält der Spieleanbieter vom Plattformbetreiber aggregierte Berichte und Auswertungen, um das angebotene Spiel zu verbessern und um das Spiel an die Nutzerbedürfnisse anpassen zu können. Diesen Auswertungen liegen Analysen der (nur) den sozialen Netzwerken vorliegenden Daten zu Grunde (wie z.B. Geschlecht, Alter und Land, in dem sich der Nutzer beim Spielen aufhält, Anzahl der Mitspieler etc.). Da die Spieleanbieter jedoch keinen Zugriff auf die Account-Daten der Plattform haben, ist ihnen insoweit ein Rückschluss auf einzelne Nutzer*innen nicht möglich.

Vor diesem Hintergrund können solche Auswertungen zwecks allgemeiner Optimierung und Verbesserung des Spielerlebnisses sowie zur Behebung technischer Fehler auf die berechtigten Interessen der Spieleanbieter gestützt werden. I.R.d. nach Art. 6 Abs. 1 lit. f DS-GVO durchzuführenden Interessenabwägung ist nämlich nicht nur zu berücksichtigen, dass der konkrete Nutzer für den Spieleanbieter dabei regelmäßig unerkannt bleibt, sondern dass auch der Nutzer selbst am Ende von den Anpassungen auf Basis dieser Analysen profitiert. Überwiegende entgegenstehende Interessen des Nutzers dürften daher regelmäßig nicht vorliegen.

c) Ausspielen von Werbung

Dies stößt jedoch an seine Grenze, wenn gezielt Nutzerprofile angelegt werden, um diese zu anderen Zwecken zu nutzen, ins-

22 *EuGH* MMR 2018, 591 m. Anm. *Moos/Rothkegel* = ZD 2018, 357 m. Anm. *Marosi/Matthé* und m. Anm. *Schulz* – ULD/WAK Schleswig-Holstein.

23 So etwa die „Snap Games Platform Terms", abrufbar unter: https://snap.com/de-DE/terms/snap-games-platform, die in die „Snap Developer Terms" eingebunden sind, abrufbar unter: https://snap.com/de-DE/terms/developer; für Facebook die „Entwickler-Richtlinien", abrufbar unter: https://developers.facebook.com/devpolicy/, die Bestandteil der „Plattform-Nutzungsbedingungen von Facebook" sind, abrufbar unter: https://developers.facebook.com/terms.

24 Vgl. Ziff. 3a der Snap Games Platform Terms; bei *Facebook* ergibt sich dies aus den Datenschutzpflichten, die *Facebook* den Spieleanbietern u.a. in Ziff. 3 und 4 der Plattform-Nutzungsbedingungen auferlegt.

25 Z.B. das Snap Data Processing Agreement, abrufbar unter: https://www.snap.com/de-DE/terms/data-processing-agreement.

26 Ausf. zu den Datenverarbeitungen in der Games-Branche *Bänsch/Hentsch* in dieser Beilage.

besondere zur personalisierten Werbung. Der Plattformbetreiber wertet die im Zusammenhang mit den Spielen erhaltenen Daten aus, um zielgerichtete Werbung an die Nutzer*innen ausspielen zu können, vor allem innerhalb der Spiele. Dies behalten sich die Plattformbetreiber in den Vertragsbedingungen gegenüber den Spieleanbietern zuweilen ausdrücklich vor,[27] während es den Spieleanbietern verboten ist, in den Spielen eigene Werbung zu betreiben, erst recht nicht durch Drittanbieter.[28]

Für diese Art der personalisierten Auswertung der Daten ist eine Einwilligung zu Gunsten der Plattformbetreiber erforderlich.[29] Ob diese bereits in der Einwilligung enthalten ist, die der Nutzer beim Anlegen seines Accounts in dem sozialen Netzwerk erteilt, mag bezweifelt werden, kann aus Sicht der Spieleanbieter jedoch dahinstehen.

3. Internationaler Datentransfer

Wie bei den Multiplayer-Spielen, besteht auch bei Spielen auf sozialen Netzwerken das Problem, dass die Datenverarbeitungen häufig außerhalb der EU stattfinden, sodass sich auch insoweit die o.g. Fragen aus dem *EuGH*-Urteil „Schrems II" stellen. Die Plattformanbieter haben zwar regelmäßig einen Sitz in der EU (meist Irland), lassen die Daten aber auch in den USA durch die Muttergesellschaft bzw. auf deren Servern oder in internationalen Clouds verarbeiten. Daher findet sich in den Datenschutzrichtlinien der Plattformanbieter üblicherweise zumindest der Hinweis, dass zwischen den Unternehmen die Standarddatenschutzklauseln vereinbart sind.[30] Das lässt sich zum einen aber kaum kontrollieren, zum anderen ist dadurch regelmäßig der Spieleanbieter nicht gebunden, der jedoch der Exporteur von personenbezogenen Daten sein kann. Sofern es um das Hosting der Spiele außerhalb der EU bzw. des EWR geht, wird ein Vertrag über Auftragsverarbeitung (DPA) abgeschlossen, in den auch die Standarddatenschutzklauseln einbezogen werden.[31] Insoweit finden sich allerdings keinerlei Hinweise auf die zusätzlichen Maßnahmen, die nun vom *EuGH* und dem *EDSA* zur Absicherung eines US-Transfers gefordert werden, wenn dieser Transfer durch die Standarddatenschutzklauseln abgesichert werden soll. Mehr Argumentationsspielraum bleibt, wenn die Plattformanbieter offener sind und der Spieleanbieter insoweit in den Dialog mit ihnen treten kann, um das Vorliegen geeigneter Garantien zu verifizieren.[32]

Es sprechen gute Gründe dafür, dass die o.g. Argumente auch hier greifen. Vor allem ist zusätzlich zu berücksichtigen, dass Spieler*innen, die Mitglied in einem der weltweiten sozialen Netzwerke sind und sich dort bewusst für das Spielen von etwa Facebook Instant Games oder Snap Games entscheiden, die Risiken, die damit im Hinblick auf die internationale Datenübermittlung verbunden sind, regelmäßig in Kauf nehmen. Auch dies ist Ausdruck der informationellen Selbstbestimmung des jeweiligen Spielers.[33]

IV. Zusammenfassung

Multiplayer-Spiele sind in der Regel global, weshalb personenbezogene Daten auch in Drittstaaten ohne angemessenes Datenschutzniveau übertragen werden. Dies ist möglich auf Basis einer entsprechend informierten Einwilligung bzw. soweit zur Vertragserfüllung notwendig, auch wenn es massenhaft geschieht. Entsprechendes gilt auch für die internationalen Datenübermittlungen beim Spielen von Games auf den großen, weltweit agierenden sozialen Netzwerken. Es ist Ausdruck der informationellen Selbstbestimmung des Spielers, wenn er sich bei einem solchen Netzwerk anmeldet und dort spielt, insbesondere um beim Spielen die Vorteile dieses sozialen Netzwerks nutzen zu können.

Das Erkennen von Betrugssoftware in Multiplayer-Spielern – sog. Cheats – erfordert eine Verarbeitung von personenbezogenen Daten in erheblichem Umfang. Dies kann auf die Notwendigkeit zur Vertragserfüllung oder – besser – auf berechtigte Interessen gestützt werden. Auf geeignete und angemessene technische und organisatorische Maßnahmen – auch unternehmensintern – ist zu achten. Des Betrugs überführte Spieler*innen werden vom Spiel ausgeschlossen. Bei populären Spielen ist eine große Anzahl von Spieler*innen betroffen. Die Entscheidung wird von Anti-Cheat-Technologie wenigstens vorbereitet. Die Entscheidung über die Kündigung des Spielenutzungsvertrags und Löschung des Accounts sollte von einem Menschen getroffen werden, der einen Entscheidungsspielraum hat. Details der Anti-Cheat-Technologie und ihrer Logik muss dieser nicht kennen.

Beim Spielen auf sozialen Netzwerken finden umfangreiche Datenverarbeitungen statt, zu denen auch der notwendige Datenaustausch zwischen Spieleanbieter und Plattformbetreiber gehört. Sofern dies zur Bereitstellung der Spiele geschieht, können sowohl die Datenübermittlung als auch die Datenverarbeitung durch den Spieleanbieter auf Vertragserfüllung gestützt werden. Auswertungen in bestimmtem Umfang, die nicht das persönliche Spielerverhalten analysieren und monetarisieren, sondern nur in aggregierter Form stattfinden, sind regelmäßig zur Wahrung der berechtigten Interessen der Spieleanbieter erforderlich. Das Ausspielen von personalisierter Werbung durch die Plattformbetreiber erfordert hingegen eine Einwilligung.

Verantwortlich für diese Datenverarbeitungen sind der Spieleanbieter und der Plattformbetreiber jeweils für ihren eigenen Bereich. Eine gemeinsame Verantwortlichkeit kann in Betracht kommen, wenn diese Bereiche eng miteinander verwoben sind. Je datensparsamer das Spiel von vorneherein ausgestaltet ist und je weniger Daten der Spieleanbieter über die konkreten Nutzer vom sozialen Netzwerk erhält, desto weniger dürfte von einer gemeinsamen Verantwortlichkeit auszugehen sein.

Schnell gelesen ...

- Sowohl Multiplayer-Games als auch Spiele auf sozialen Netzwerken sind meist global, sodass personenbezogene Daten auch in sog. Drittstaaten übertragen werden können. Dies kann auf Grund von Art. 49 Abs. 1 lit. a bzw. b DS-GVO (Einwilligung oder Vertragserfüllung) zulässig sein.
- Beim Einsatz von Anti-Cheat-Technologie ist auf die Besonderheiten der automatisierten Entscheidungsfindung gem. Art. 22 DS-GVO zu achten. Das gilt auch, falls von Spieler*innen Auskunftsansprüche geltend gemacht werden.

27 Ziff. 2e. der Snap Games Platform Terms; bei *Facebook* ergibt sich dies aus dem Gesamtzusammenhang der Vorgaben in den Plattform-Nutzungsbedingungen und Entwickler-Richtlinien, insb. unter Berücksichtigung der Datenschutzrichtlinie ggü. den Nutzer*innen, in der die Datennutzung zu Werbezwecken ausführlich erläutert wird, abrufbar unter: https://www.facebook.com/about/privacy.

28 Ziff. 2e (letzter Satz) der Snap Games Platform Terms, Ziff. 7: Abs. 4b. der Facebook Entwickler-Richtlinien; bei *Facebook* ist lediglich die Einbindung des Facebook Audience Network gestattet.

29 Ausf. dazu *Baumgartner/Hansch*, ZD 2020, 435.

30 So z.B. in den Datenschutz-Informationen für Unternehmen zum Thema Datenübermittlung, abrufbar unter: https://de-de.facebook.com/business/gdpr.

31 Vgl. das Snap DPA, dort Ziffer 6 „Data Transfers", abrufbar unter: https://www.snap.com/de-DE/terms/data-processing-agreement.

32 So verweist die *Snap Group Limited* in ihrem DPA darauf, dass ein Transfer personenbezogener Daten von Betroffenen aus der EU oder UK nur durchgeführt werde, wenn die Anforderungen aus Art. 44 bis 47 DS-GVO erfüllt sind oder eine der Ausnahmeregelungen in Art. 49 DS-GVO vorliegt.

33 Vgl. zu eCommerce: *Gabel*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 49 Rn. 7-9; *Lange/Filip*, in: BeckOK DatenschutzR (o. Fußn. 11), Art. 49, Rn. 13-19; *Schröder*, in: Kühling/Buchner (o. Fußn. 18), Art. 49 Rn. 19a.

■ Die üblichen Datenverarbeitungen im Rahmen dieser Spiele können regelmäßig auf Vertragserfüllung oder berechtigte Interessen gestützt werden. Einwilligungen zu Gunsten der Spieleanbieter sind in der Regel nicht erforderlich.

■ Verantwortlich sind nicht nur die Spieleanbieter, sondern auch die jeweiligen Plattformbetreiber für ihre eigenen Datenverarbeitungen im sozialen Netzwerk. Eine gemeinsame Verantwortlichkeit kann in Betracht kommen, muss aber nicht zwingend sein.

Dr. Andreas Lober
ist Partner der BEITEN BURKHARDT Rechtsanwaltsgesellschaft in Frankfurt/M. und Co-Leiter der Praxisgruppe IP/IT/Medien.

Susanne Klein, LL.M.,
ist Partnerin der BEITEN BURKHARDT Rechtsanwaltsgesellschaft in Frankfurt/M. und Fachanwältin für Informationstechnologierecht sowie zertifizierte Datenschutzbeauftragte.

AXEL VON WALTER

Nutzerdaten, KI und automatisierte Entscheidungsfindung in Games

Datenschutzrechtliche Anforderungen an den Einsatz von automatisierter Entscheidungsfindung in Videospielen

Machine Learning

Künstliche Intelligenz (KI) spielt natürlich auch für Videospiele und deren Monetarisierung zunehmend eine größere Rolle. Die Branche ist ein Innovationstreiber und setzt schon länger auf Machine Learning und KI, um die Spielwelten noch glaubwürdiger und das Spielerlebnis noch authentischer zu gestalten. Das schließt auch mit ein, dass regelwidrige Beeinflussungen des Spiels (sog. Cheats) mit KI intelligenter bekämpft werden können. Die KI erkennt und entscheidet oder erkennt und unterstützt Entscheidungen. Der Beitrag legt den Schwerpunkt auf die spezifischen datenschtzrechtlichen Anforderungen an den Einsatz von KI und automatisierter Entscheidungsfindung im Umfeld von Videospielen. Lesedauer: 24 Minuten

I. Künstliche Intelligenz und Games

Es ist ein Allgemeinplatz, dass Künstliche Intelligenz (KI) für moderne Videospiele eine vitale Rolle spielt – dies auch in verschiedenen Dimensionen des Produkts und im Verhältnis zum Nutzer. Nach einem kurzen Streif durch die Haupteinsatzgebiete der KI in Videospielen will dieser Beitrag den Schwerpunkt auf die datenschutzrechtlichen Anforderungen (insbesondere Art. 22 DSGVO) an die automatisierte Entscheidungsfindung in Videospielen legen.

1. KI und Gameplay

Zunächst ist der Einfluss der KI auf das Gameplay selbst. Die meisten virtuellen Realitäten und Game-Settings in modernen Videospiele werden sowohl von menschengesteuerten als auch von Nicht-Spieler-Charakteren (Non Player Characters – NPCs) bewohnt. NPCs werden zunehmend als KI-gesteuerte virtuelle Agenten, neutrale Charaktere, feindliche Gegner oder freundliche Teamkameraden eingesetzt. Die Qualität der NPCs beeinflussen das Gameplay und die Spielerfahrung des Nutzers maßgeblich. Die Anforderungen an das entsprechende KI-System sind hoch, da für die Spielerfahrung der Nutzer*innen nicht die eigene Zielerreichung der NPCs der Schlüssel ist, sondern der Spaß an der Interaktion zwischen Nutzer und NPCs. Die Spielentscheidungen der NPCs selbst beruhen auf automatisierter Entscheidungsfindung.

Um das auf KI-basierende Verhalten der NPCs stetig zu verbessern, setzen Publisher auch auf Machine Learning, basierend auf dem Spiel- und Kommunikationsverhalten der Nutzer*innen. Das systematische Sammeln und Auswerten von Verhaltensinformationen kann den selbstlernenden Algorithmus für die Entscheidungen der NPCs im Gameplay laufend verbessern. Das Sammeln der nutzerbezogenen Verhaltensinformationen dient dem Machine Learning, also der Verbesserung der KI. Davon zu unterscheiden ist die Anwendung der KI, z.B. zur automatisierten Entscheidungsfindung.

2. KI und Game-Testing

Ein weiteres Feld für den Einsatz von KI im Kontext von Videospielen ist das Game-Testing. Je komplexer die Spielwelten und Interaktionen zwischen Nutzer*innen, anderen Spielern und NPCs in Videospielen gestaltet sind, desto herausfordernder ist das Game-Testing in der Qualitätssicherung. Die Komplexität des automatisierten Testens geht hier weit über das bloße Software-Testen hinaus. Im Vergleich zur allgemeinen Softwareentwicklung müssen bei der Qualitätssicherung von Videospielen mehrere zusätzliche Aspekte berücksichtigt werden, wie Testen des Spaßfaktors, Testen der Spielbalance, Testen der einzelnen Spielebenen/-welten usw. Das KI-basierte Game-Testing selbst ist ein interner Prozess bei der Entwicklung Weiterentwicklung von Videospielen und weist in der Regel keinen echten Nutzerbezug i.S.e. Verarbeitung von nutzerbezogenen Daten auf.[1]

3. KI und Betrugsabwehr/Anti-Cheat

Das praktisch besonders bedeutsame Anwendungsgebiet der KI im Verhältnis zwischen Publisher und Nutzer*innen des Spiels ist die Betrugsabwehr bzw. das Verfahren des Anti-Cheat. Dabei werden selbstlernende automatisierte Betrugserkennungsverfahren sowohl im Gameplay selbst als auch in der Zahlungsabwicklung eingesetzt. Die Betrugserkennung in der Zahlungsabwicklung dient dabei der Integrität der Bezahlung für die Nutzung

1 Deswegen soll das Game-Testing hier nur als weiteres Beispiel für ein Einsatzgebiet der KI für Videospiele erwähnt sein, wird aber für die weitere Erörterung der datenschutzrechtlichen Aspekte automatisierter Entscheidungsfindung keine größere Rolle spielen.

des Spiels oder für In-Game-Käufe digitaler Güter oder der Einhaltung anderer regulatorischer Anforderungen im Zahlungsverkehr. Die Betrugserkennung unterscheidet sich dabei auch bei videospielbasierten Geschäftsmodellen nicht wesentlich von solchen anderer Telemedienanbieter oder im eCommerce.

Neben den zahlungsbezogenen Erkennungsverfahren kommen vor allem für die Integrität des Spiels KI-basierte Verfahren zur Erkennung von Manipulationen und unlauteren Beeinflussungen des Spielablaufs – sog. Cheats – zum Einsatz. Der Schutz des Spielablaufs vor Cheats ist für das Spiel, die Nutzer*innen und damit auch für den Publisher von vitalem Interesse. Der Publisher lebt von dem Vertrauen der Nutzer*innen in das authentische und unbeeinflusste Spielerlebnis. Knapp gesagt: Wird dieses Vertrauen nur durch den Verdacht der relevanten Manipulation durch Dritte erschüttert, wenden sich Nutzer*innen von dem Spiel ab und das Geschäftskonzept des Publishers von Spielen, die in die Entwicklung der Spiele größere Budgets als die der großen Hollywoodfilmproduktionen investieren, geht nicht auf.

Zu den Methoden und Erkennungsverfahren bei Anti-Cheat-Maßnahmen sind nur wenige Details öffentlich verfügbar. Nachvollziehbare Geheimhaltungsinteressen der Publisher sorgen dafür, dass viele Methoden im Detail noch nicht oder nie öffentlich werden. Zudem entwickeln sich die Erkennungstechniken ständig weiter. Publisher entwickeln neue Methoden, um Cheater zu erkennen, während alte Methoden wirkungslos und redundant werden. Ganz generell können zwei Kategorien von Erkennungsmethoden unterschieden werden. Während Client-basierte Methoden eher auf die technische Entdeckung und Verhinderung von unlauterer Spielbeeinflussung auf der persönlichen Hardware des Spielers (Client) zielen, gehen Server-basierte Methoden auf die Auswertung des persönlichen (Spiel-)-Verhaltens, das serverseitig geloggt und ausgewertet werden kann.[2] Beide Methoden können relevante personenbezogene Daten liefern, die Grundlage für den Einsatz von KI und für automatisierte Entscheidungsfindung sein können.

4. Teilbereich der KI: Die automatisierte Entscheidungsfindung

So vielfältig die Anwendungsgebiete der Künstlichen Intelligenz sind, sind insbesondere Verfahren zur automatisierten Entscheidungsfindung in der Praxis von großer Relevanz für Publisher. Bei der ausschließlich automatisierten Entscheidungsfindung handelt es sich um die Fähigkeit, Entscheidungen ohne direkte Beteiligung einer Person mithilfe technischer Mittel zu treffen.[3] Verfahren zur automatisierten Entscheidungsfindung werden auch ADM-Verfahren genannt.[4] Im Rahmen der Grundmerkmale, die „intelligente" Anwendungen charakterisieren – Wahrnehmen, Verstehen, Handeln und Lernen – ist die automatisierte Entscheidungsfindung ein Teilbereich des Merkmals „Handeln". ADM-Systeme führen basierend auf dem bisherigen algorithmisch abgebildeten Wissen als maschinelle Handlung eine Entscheidung herbei und setzen die anderen Elemente als Informationserfassung und -verarbeitung voraus. Die Vorteile für den Einsatz von KI zur automatisierten Entscheidungsfindung liegen auf der Hand. ADM-Systeme können eine ungleich größere Menge an Informationen berücksichtigen und im Idealfall eine neutrale und rein informationsbasierte Entscheidung treffen. ADM-Systeme legen also in der praktischen Anwendung schnelle, kostengünstige und vielleicht bessere Entscheidungen nahe. Aber auch ADM-Systeme haben Schwächen und die maschinell getroffenen Entscheidungen können spürbare Konsequenzen für Menschen haben.

Die Entscheidungsfindung von ADM-Systemen ist in der Praxis meist wenig transparent. Zum einen, weil die Entscheidungen in einer systemischen Blackbox getroffen werden.[5] Zum anderen, weil die zu Grunde liegenden Algorithmen als Geschäftsgeheimnis der entwickelnden Unternehmen gut gehütet bleiben. Eine ungeeignete Datenbasis kann zu verdeckter Diskriminierung führen und weitreichende Folgen für die Lebensumstände von Menschen haben. Es gibt einzelne spezielle gesetzliche Regelungen zur allgemeinen Vermeidung von Diskriminierung. Insbesondere die DS-GVO will jedoch Menschen grundsätzlich davor schützen, in ihrem Lebens- und Sozialbereich Objekt einer vollständig automatisierten Entscheidung von Maschinen zu werden.[6] Dem nachfolgend will der Beitrag die datenschutzrechtliche Perspektive auf den Einsatz von ADM-Systemen im Bereich der Videospiele näher ausleuchten.

II. Automatisierte Entscheidungen im Einzelfall

Die grundlegende Regelung für die Frage der Zulässigkeit von ADM-Systemen findet sich in der DS-GVO in Art. 22 Abs. 1.[7] Danach hat jeder das Recht „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt."

In Absatz 2 werden automatisierte Entscheidungen, die für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sind (lit. a) und automatisierte Entscheidungen mit ausdrücklicher Einwilligung der betroffenen Person (lit. c) von dem Verbot aus Absatz 1 ausgenommen. Absatz 4 enthält eine Rückausnahme für besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO.

Generell verbietet Art. 22 Abs. 1 DS-GVO eine vollständig automatisierte Entscheidung im Einzelfall, welche rechtliche Wirkung entfaltet oder in ähnlicher Weise erheblich beeinträchtigt (Grundsatz). Von diesem Grundsatz gibt es Ausnahmen. Wenn und soweit eine Ausnahme von dem Grundsatz Anwendung findet, müssen Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person implementiert sein, einschließlich der Information über die Verarbeitung sowie der Möglichkeit des menschlichen Eingreifens in die Entscheidungsfindung.[8]

Die für eine automatisierte Entscheidungsfindung notwendige Datenverarbeitung kann nur über die Erlaubnistatbestände des

2 Fragen in Zusammenhang mit der Client-basierten Datenauswertung und der RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) können für diesen Beitrag ausgeblendet werden, da es hier um die automatisierte Entscheidungsfindung basierend auf den erhobenen Daten geht.

3 Vgl. die Definition in WP 251rev.01 „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679", S. 8.

4 „ADM" steht für Algorithmic Decision Making, algorithmische Entscheidungsfindung.

5 ADM-Systeme treffen Entscheidungen in Systemen, die aus mehreren Schichten (Layern) von künstlichen „Neuronen" bestehen und jede Schicht selbstlernende Algorithmen anwendet, sodass eine Operation, die mehrere Layer durchläuft für den Menschen kaum nachvollziehbar ist und man deswegen bei KI-Systemen auch von „Blackbox" spricht; s. zu den technischen Hintergründen der KI und den Systemen *Stiemerling*, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 2.1, Rn. 6 ff.

6 Vgl. Erwägungsgrund 71 S. 1 DS-GVO.

7 Art. 9 Abs. 1 lit. a der Konvention 108 des Europarates enthält in der revidierten Fassung nach der Annahme des Protokolls von 2018 ebenfalls ein Verbot, Personen einer Entscheidung zu unterwerfen, wenn die Entscheidung ausschließlich automatisiert erfolgt. Das Verbot gilt indes nur, wenn die Entscheidung erhebliche Auswirkungen auf die betroffene Person hat.

8 Vgl. Erwägungsgrund 71 S. 4: „In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung."

Art. 6 DS-GVO gerechtfertigt werden. Bei Art. 22 Abs. 1 DS-GVO handelt es sich nicht um eine legitimierende Rechtsgrundlage für automatisierte Entscheidungsfindung, sondern vielmehr um eine ergänzende Einschränkung für die vollautomatisierte Verarbeitung von personenbezogenen Daten für den Fall, dass die Verarbeitung gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder vergleichbar erheblich beeinträchtigt.

Art. 22 DS-GVO ist keine Beschränkung der Künstlichen Intelligenz selbst. Die Regelung ist vielmehr lediglich eine Beschränkung der Einsatzwirkung von Künstlicher Intelligenz.

Entscheidend für die Frage, inwieweit automatisierte Entscheidungen im Umfeld von Videospielen im Anwendungsbereich der DS-GVO eingesetzt werden können ist, ob es sich um eine vollständig automatisierte Entscheidung mit relevanter Wirkung für den Betroffenen handelt oder eine gesetzliche Ausnahme des grundsätzlichen Verbots vorliegt.

1. Automatisierte Entscheidung

Da das Verbot des Art. 22 DS-GVO die betroffenen Personen davor bewahren will, zum Objekt von Maschinenentscheidungen zu werden, greift es nur in den Fällen, in welchen maschinelle – mithin automatisierte – Entscheidungen ohne jeglichen menschlichen Entscheidungseinfluss getroffen werden. Anders gewendet ist für das Verbot einer Datenverarbeitung kein Raum, wenn entweder schon keine Entscheidung getroffen wird oder der Mensch an der Datenverarbeitung letztendlich doch relevant mitwirkt.

a) Entscheidung oder bloße Ausführung?

Gegenstand des Verbots in Art. 22 Abs. 1 DS-GVO sind nur „Entscheidungen". Der Begriff der Entscheidung ist in der DS-GVO nicht definiert. Keine Entscheidung liegt vor, wenn vorab zwischen der betroffenen Person und dem verantwortlichen vereinbarte „Wenn-dann"-Regeln maschinell abgearbeitet werden. Das automatisierte Ausführen von vorher gemeinsam festgelegten Folgen ist keine Entscheidung, weil es letztendlich an einer autonomen Bewertung, Abwägung und Ermessensausübung fehlt.[9]

Sofern der Publisher innerhalb des Gameplays oder bei Anti-Cheat-Maßnahmen lediglich vorher mit dem Nutzer vertraglich festgelegte Wenn-dann-Mechanismen maschinell umsetzt, liegt in dieser automatisierten Datenverarbeitung schon keine Entscheidung i.S.d. Art. 22 Abs. 1 DS-GVO. Das bezieht sich auf binäre Entscheidungsstrukturen, die maschinell abgearbeitet werden. Schließt der Publisher z.B. in seine Nutzungsbedingungen Spielregeln mit ein, die einem binären Verstoß/Sanktionsprinzip folgen, kann in der bloßen automatisierten Exekution dieser vorab festgelegten Regeln keine automatisierte „Entscheidung" liegen. Sofern jedoch innerhalb der Datenverarbeitung KI-basierte Bewertungen eine Rolle spielen, die im menschlichen Entscheidungsprozess als Ermessensausübung bezeichnet würden, handelt es sich, dem Schutzzweck der Norm folgend, um eine Entscheidung i.S.d. Art. 22 DS-GVO.

b) Der fehlende menschliche Faktor

Dem Verbot des Art. 22 Abs. 1 DS-GVO unterliegen lediglich Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen. Nur dann fehlt es an einer einflussnehmenden Mitwirkung eines Menschen und die Entscheidung erfolgt rein maschinell. Um für eine Einbeziehung eines Menschen bei der Entscheidung zu sorgen, darf die Mitwirkung des Menschen nach der herrschenden Auffassung bei der Entscheidung nicht bloße Förmelei sein. Für die menschliche Beurteilung und Letztentscheidung muss genügend Spielraum bleiben.[10] Letztendlich muss der Mensch weitere Aspekte in seine Entscheidung mit einbeziehen. Denn auch eine menschliche Entscheidung, die schlicht den maschinellen „Entscheidungsvorschlag" umsetzt, beruht letztendlich auch ausschließlich auf einer maschinellen Verarbeitung. Auch wenn also die automatisierte Verarbeitung und die Entscheidungshandlung nicht zusammenfallen, kann insoweit eine automatisierte Entscheidung i.S.d. Art. 22 Abs. 1 DS-GVO vorliegen. Anders liegt es bei einer bloßen Entscheidungsunterstützung oder Entscheidungsvorbereitung durch intelligente Systeme. Art. 22 DS-GVO zielt nicht darauf ab, die Entscheidungsunterstützung und -vorbereitung durch automatisierte Verfahren zu verhindern.[11] Unterstützt die Künstliche Intelligenz den Menschen in seiner Entscheidungsfindung, liegt keine ausschließliche automatisierte Entscheidung vor. Unterstützt die KI den Menschen, indem sie die Entscheidung mit erheblichen rechtlichen oder sonstigen Wirkungen für ihn trifft, unterfällt diese Anwendung dem grundsätzlichen Verbot des Art. 22 Abs. 1 DS-GVO. Es ist in der Abgrenzung häufig eine Frage des Einzelfalls, der allerdings gerade im Zusammenhang mit der Cheat-Erkennung eine praktisch hohe Relevanz hat. Denn gerade in der Cheat-Abwehr sind Publisher auf automatisierte Erkennungssysteme angewiesen, die bei Vorliegen eines begründeten Cheat-Verdachts zu Konsequenzen für den Spieler – von zeitlichen Sperren bis hin zur Kündigung des Vertragsverhältnisses – führen können. Hier bereiten oder nehmen Systeme Entscheidungen vor.

Sofern das Anti-Cheat-Team des Publishers das Recht hat, die von dem automatisierten System vorgeschlagene Verbotsentscheidung aufzuheben, hat der menschliche Faktor bestimmenden Charakter und es liegt kein Fall des Art. 22 Abs. 1 DS-GVO vor. Falls das Anti-Cheat-Team des Publishers nur einen begrenzten Einfluss hat, bevor eine vorübergehende Sperre verhängt wird, z.B. nur das Recht hat, zu überprüfen, ob die vorgeschlagene Entscheidung zur Sperre frei von offensichtlichen Fehlern ist, wird dies nicht als ausreichende menschliche Beteiligung qualifiziert werden.

Allerdings sind auch solche Entscheidungen, die auf menschlichem Einfluss Dritter beruhen, keine ausschließlich maschinellen Entscheidungen i.S.d. Art. 22 Abs. 1 DS-GVO. Beruht z.B. eine Entscheidung des Systems, ein Nutzerkonto oder Spielerprofil zu sperren, allein auf Nutzerbeschwerden, liegt keine „automatisierte Entscheidung" vor. Die Anti-Cheat-Logik setzt hier lediglich technisch die Entscheidung von Menschen durch. Die Sperrentscheidung beruht hier auf einem Zusammenwirken der vorab definierten Kriterien des Publishers mit der Entscheidung der Massen (z.B. andere Spieler, die Beschwerden/Blocking-Vorschläge eingereicht haben). Hier wird die Entscheidung letztlich nicht von einem Menschen, sondern von einer Zahl N von Menschen ausgelöst, mithin wird der Nutzer gerade nicht zum Objekt einer ausschließlich maschinellen Entscheidung.

2. Relevante Auswirkung für die betroffene Person

Einigkeit besteht darüber, dass nur solche automatisierten Entscheidungen vom Verbot des Art. 22 Abs. 1 DS-GVO umfasst sein sollen, die eine relevante Auswirkung für die betroffene Person haben. Nach dem Wortlaut der Vorschrift genügt alternativ zum einen (a)) jede „rechtliche Wirkung" oder zum anderen (b)) eine „erhebliche" Beeinträchtigung in „ähnlicher Weise".

a) Rechtliche Wirkung

Rechtliche Wirkungen sollen nur solche Entscheidungen haben, die eine Rechtsposition begründen, ändern oder aufhe-

9 Simitis/Hornung/Spiecker gen. Döhmann/*Scholz*, DSGVO, Art. 22 Rn. 17, 18 macht dies auch an dem Begriff des „Unterworfenseins" fest.

10 Vgl. auch *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 22.

11 Vgl. Paal/Pauly/*Martini*, Datenschutzgrundverordnung, 2. Aufl., Art. 22 Rn. 20.

ben.[12] Das kann den rechtlichen Status einer Person genauso betreffen, wie auch die Rechte einer Person aus einem Vertragsverhältnis.[13]

Letztlich kommt eine echte rechtliche Wirkung im Verhältnis Publisher und Nutzer in der Praxis nur auf der Ebene des Nutzungsvertrags in Betracht. Es spielt dabei keine Rolle, ob das Nutzungsverhältnis entgeltlich oder unentgeltlich ausgestaltet ist. Es kommt lediglich auf den rechtlichen Effekt, also auf das Bestehen oder Nichtbestehen von Ansprüchen oder Rechtspositionen an. Beruht also die Entscheidung, ein Vertragsverhältnis zu beenden, ausschließlich auf einer automatisierten Entscheidung, wird dem eine rechtliche Wirkung zuzuschreiben sein und das Verbot des Art. 22 Abs. 1 DS-GVO greift. In der Praxis ist aber der Vertragsbeendigung zunächst eine Verwarnung oder eine vorübergehende Sperrung des Nutzerkontos vorausgegangen. Es bleibt strittig, ob die Verwarnung – der ja i.R.e. außerordentlichen Vertragskündigung entsprechend § 626 BGB eine eigene rechtliche Bedeutung zukommt – schon eine echte rechtliche Wirkung hat oder nicht. Auch die vorübergehende Sperrung eines Nutzerkontos könnte mit rechtlicher Wirkung angesehen werden, denn darin liegt die zumindest vorübergehende Leistungsverweigerung des Publishers aus dem vertraglichen Nutzungsverhältnis.

b) Ähnliche erhebliche Beeinträchtigungen

Letztendlich reichen aber auch vergleichbare erhebliche Beeinträchtigungen für ein Verbot der Datenverarbeitung nach Art. 22 Abs. 1 DS-GVO aus. Welche Wirkung für eine Person als erheblich i.S.d. Art. 20 Abs. 1 DS-GVO anzusehen ist, ist schwer zu definieren.[14] Sofern die automatisierte Entscheidung geeignet ist, die Umstände, das Verhalten oder die Entscheidungen der betroffenen Person zu beeinträchtigen, die betroffene Person über einen längeren Zeitraum oder dauerhaft beeinträchtigt oder im schlimmsten Fall zum Ausschluss oder zur Diskriminierung führt, soll jedenfalls die Erheblichkeitsschwelle überschritten sein. Das trifft für Entscheidungen, die sich auf finanzielle Aspekte einer Person auswirken, Entscheidungen über den Zugang zu Gesundheitsdienstleistungen, Entscheidungen über den Zugang zu Arbeitsplätzen oder Entscheidungen über den Zugang zu Bildung zu.[15]

Nach einer anderen Auffassung ergebe sich aus dem Wort „beeinträchtigt", dass grundsätzlich nur belastende Entscheidungen, nicht aber begünstigende Entscheidungen von Art. 22 DS-GVO umfasst sein sollen.[16] Folgt man dieser Auffassung, hängt die Zulässigkeit der automatisierten Entscheidung letztendlich vom Ergebnis des Verarbeitungsprozesses ab: Ist die maschinelle Entscheidung für den Betroffenen positiv, fehlt es an der „beeinträchtigenden „Wirkung und die automatisierte Entscheidungsfindung ist letztendlich im Einklang mit Art. 22 DS-GVO. Fällt die maschinelle Entscheidung negativ aus, ergibt sich daraus die Beeinträchtigung und damit die Unzulässigkeit. Richtigerweise muss man aber davon ausgehen, dass alle automatisierten Entscheidungen mit erheblicher Wirkung unabhängig von ihrem Ergebnis in den Verbotsbereich des Art. 22 Abs. 1 DS-GVO fallen. Das Wortlautargument aus der deutschen Sprachfassung der DS-GVO, dass auf dem Wort „beeinträchtigt" basiert, wird sowohl durch die englische[17] als auch durch die französische[18] Sprachfassung der DS-GVO deutlich geschwächt. Die Begriffe „affect" bzw. „l'affectant" können dort auch als „betreffen" oder „berühren" verstanden werden. Letztlich sprechen auch Sinn und Zweck der Vorschrift für ein neutrales Verständnis und die Einbeziehung aller automatisierten Entscheidungen mit wesentlichen Auswirkungen auf die betroffenen Personen. Ziel der Vorschrift ist es, den Menschen in seinen wesentlichen die Lebensumstände bestimmenden Aspekten, nicht Objekt einer rein maschinellen Entscheidung zu werden. Im Kern geht es darum, dass die Person nicht zum „bloßen Objekt von Computeroperationen degradiert" und die Verantwortung für Entscheidungen über Menschen nicht anonym Computersystemen zugeschrieben werden darf.[19]

Deswegen kann man letztendlich schon trefflich darüber streiten, ob eine automatisierte Entscheidung im Kontext eines Videospiels überhaupt geeignet ist, die Erheblichkeitsschwelle des Art. 22 Abs. 1 DS-GVO zu überschreiten. Nur ausnahmsweise werden Entscheidungen das Gameplay und die Teilhabemöglichkeit die wesentlichen Lebensumstände des Nutzers betreffen. Das mag bei Spieler*innen in gut dotierten eSport-Tournaments der Fall sein. Für den Gelegenheitsspieler wird es weder um erhebliche finanzielle Aspekte noch um den Zugang zu Erwerbschancen gehen.

Zuletzt ist auch offenkundig, dass die systemseitigen Entscheidungen für das Spielverhalten der NPCs im Spiel selbst keine „erheblichen Beeinträchtigungen" im Rechtssinne darstellen und damit alle auf KI basierenden Spielentscheidungen, die produktinherent sind und von den Spieler*innen auch als Grundlage für ein möglichst authentisches Gameplay erwartet werden, selbstverständlich nicht dem Verbot des Art. 22 Abs. 1 DS-GVO unterliegen – auch wenn der KI-gesteuerte Endgegner den Nutzer letztendlich „by machine learning" besiegt.

3. Ausnahmen vom Verbot der automatisierten Entscheidungsfindung

Von dem grundsätzlichen Verbot der automatisierten Entscheidung mit relevanter Auswirkung für die betroffene Person bestehen auch gesetzliche Ausnahmen, die für die Nutzung von ADM-Systemen im Kontext von Videospielen tragfähig sein können.

a) Vertragsbegründung und -durchführung

Nach Art. 22 Abs. 2 lit. a DS-GVO gilt das Verbot der automatisierten Entscheidungsfindung z.B. nicht, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Diese Ausnahme hat hohe praktische Relevanz, will man mithilfe der KI Verträge anbahnen, abschließen und leben. Die Ausnahmeregelung ist grundsätzlich auf alle Verträge zwischen der betroffenen Person und dem Verantwortlichen anwendbar. Die automatisierte Entscheidungsfindung muss auch nicht den Hauptleistungsgegenstand der Vereinbarung bilden, sondern kann die Vertragsdurchführung i.Ü. erleichtern oder gar ermöglichen. Gleichwohl ist dieser Ausnahmetatbestand auf erforderliche automatisierte Entscheidungen beschränkt. Weil es sich bei den Regelungen in Art. 22 Abs. 2 DS-GVO um Ausnahmen von dem grundsätzlichen Verbot in Art. 22 Abs. 1 DS-GVO handelt, ist das Tatbestandsmerkmal der Erforderlich-

12 Gola/*Schulz*, DS-GVO, 2. Aufl., Art. 22, Rn. 22.
13 Vgl. *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 23.
14 *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 23.
15 Vgl. die Beispiele der *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 24.
16 Vgl. *Schulz* (o. Fußn. 12); Taeger/Gabel/*Taeger*, DSGVO, 3. Aufl., Art. 22 Rn. 47.
17 "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly *affects* him or her." [Hervorhebung durch Autor]
18 "La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou *l'affectant* de manière significative de façon similaire." [Hervorhebung durch Autor]
19 Dammann/Simmitis, Datenschutzrichtlinie, Art. 15 Rn. 2; Kühling/Buchner/*Buchner*, DS-GVO, 2. Aufl., Art. 22 Rn. 11; vgl. auch die Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 3.4.2019 („Hambacher Erklärung zur Künstlichen Intelligenz"), S 3.

keit eng zu verstehen. Der Verantwortliche muss berücksichtigen, ob ein weniger in die Privatsphäre eingreifendes Verfahren angewandt werden könnte.[20] Auch i.R.d. Durchführung von Vertragsverhältnissen können automatisierte Entscheidungen erforderlich sein, insbesondere dann, wenn in Sekundenbruchteilen Entscheidungen notwendig sind. Fraglich ist allerdings, ob Betrugsabwehr und Anti-Cheat-Verfahren als für die Vertragsdurchführung erforderlich i.S.d. Ausnahmeregelung angesehen werden können. Für die Betrugsabwehr wird es schwieriger, die Erforderlichkeit zu begründen, wie auch bei anderen Geschäftsmodellen Maßnahmen zur Betrugsvermeidung bei der Abrechnung der Leistungen (Kreditkarten-Betrug) keine für die Vertragsdurchführung erforderliche Maßnahme gesehen wird. Für Videospiele und der In-Game-Cheat-Abwehr liegt der Fall jedoch anders. Wie der *BGH* bereits entschieden hat, ist die Wettbewerbsgleichheit in Multiplayer-Spielen integraler Erfolgsfaktor für das Spiel.[21] Ist die Chancen- und Wettbewerbsgleichheit im Spiel nicht sichergestellt, werden sich die Spieler*innen von dem Spiel abwenden, so der *BGH*. Folgt man dieser Feststellung, entspricht es der Erwartung der Spieler*innen, dass in dem Spiel Chancen- und Wettbewerbsgleichheit entsprechend der geltenden Spiel- und Nutzungsbedingungen herrschen. Auch der manipulierende Spieler nimmt in Erwartung, dass jedenfalls die Mehrzahl der Mitspieler*innen sich an die geltenden Wettbewerbsbestimmungen hält, an dem Spiel teil. Mithin kann das Verfahren zum Anti-Cheat als für die Vertragserfüllung insgesamt erforderliche Datenverarbeitung und damit den Ausnahmetatbestand des Art. 22 Abs. 2 lit. a DS-GVO erfüllt angesehen werden.

b) Einwilligung in ADM

Neben den gesetzlichen Ausnahmetatbeständen kann die betroffene Person in die Datenverarbeitung zur automatisierten Entscheidung „ausdrücklich" nach Art. 22 Abs. 2 lit. c DS-GVO einwilligen. Die Anforderungen und Bedingungen für die Einwilligung aus Art. 7 DS-GVO finden auch hier Anwendung. Zusätzlich fordert die gesetzliche Ausnahme eine „ausdrückliche Einwilligung". Die Einwilligung muss also ausdrücklich auf eine oder mehrere konkrete automatisierte Entscheidungsprozesse bezogen sein. Nach der Gesetzessystematik des Art. 22 DS-GVO entbindet die ausdrückliche Einwilligung zur automatisierten Entscheidungsfindung nach Art. 22 Abs. 2 lit. c DS-GVO lediglich von dem grundsätzlichen Verbot der automatisierten Entscheidung mit erheblichen Auswirkungen für die betroffene Person. Diese Einwilligung muss von den einwilligungsbasierten Erlaubnistatbeständen des Art. 6 DS-GVO unterschieden werden. Es ist eine Frage der konkreten Formulierung der Einwilligung, ob diese Einwilligung doppelt legitimierende Wirkung haben kann. Zum einen als Rechtsgrundlage für die Datenverarbeitung als solche nach Art. 6 Abs. 1 lit. a DS-GVO und zum anderen als Grundlage für automatisierte Entscheidungen im Rahmen dieser Datenverarbeitung. Denkbar wäre auch, die Datenverarbeitung auf eine gesetzliche Rechtfertigung im Katalog der Art. 6 und 9 DS-GVO zu stützen und lediglich die Form der automatisierten Entscheidungsfindung auf Einwilligungsbasis zu ermöglichen. Die Einwilligung ist – wie alle Einwilligungen – grundsätzlich jederzeit frei widerruflich.

4. Kein ADM bei Daten über Weltanschauung, Körper und Gesundheit

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) dürfen grundsätzlich nicht für Entscheidungen auf Grundlage einer automatisierten Verarbeitung herangezogen werden, auch dann nicht, wenn eine gesetzliche Ausnahme des Art. 22 Abs. 2 DS-GVO greift. Das betrifft alle personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, wie auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DS-GVO). Sofern also automatisierte und relevante automatisierte Entscheidungen auf Körperdaten oder Daten über Weltanschauung basieren, unterliegen diese Datenverarbeitungsvorgänge dem Verbot des Art. 22 Abs. 1 DS-GVO und können nicht über die gesetzlichen Ausnahmen des Art. 22 Abs. 2 DS-GVO legitimiert werden. Was auf den ersten Blick im Games-Kontext fernliegend scheint, ist es auf den zweiten Blick nicht: Denn z.B. automatisierte Verfahren zur Erkennung von Hate Speech können auf Informationen zur Weltanschauung der betroffenen Person beruhen, wie auch im Bereich eSports und Competitive Gaming in Echtzeit die Erhebung und Auswertung von körperbezogenen Informationen, wie Pulsschlag oder Augenbewegungen denkbar sind.

Besondere Kategorien personenbezogener Daten können allerdings auch dann in automatisierte Entscheidungen einfließen, soweit die ausdrückliche Einwilligung in die Verarbeitung besonderer Datenkategorien vorliegt.

5. Angemessene Schutzmaßnahmen für betroffene Personen

Sofern die Grundlage für die automatisierte Entscheidung entweder ein Vertragsverhältnis (Art. 22 Abs. 2 lit. a DS-GVO) oder eine Einwilligung ist (Art. 20 Abs. 2 lit. c DS-GVO), hat der Verantwortliche gem. Art. 22 Abs. 3 DS-GVO angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Dazu soll mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehören.[22] Nach Erwägungsgrund 71 müssen die Garantien für die Verarbeitung zur automatisierten Entscheidungsfindung in jedem Fall zusätzlich eine spezifische Unterrichtung der betroffenen Person umfassen. Die Transparenz bei der Verarbeitung und automatisierten Entscheidung ist essenziell, um den grundlegenden Bedenken gegen automatisierte Entscheidungen entgegentreten zu können.

Hierher gehören auch die Maßnahmen zur Vermeidung von Fehlern in der Entscheidungsfindung und insbesondere zur Vermeidung von Diskriminierung. Das setzt schon viel früher an, denn Grundlage für automatisierte Entscheidungen sind letztendlich die Trainingsdaten sowie die Datenbasis, auf der das ADM-System arbeitet. Ist die Auswahl der Trainingsdaten allerdings schlecht, wird auch das Ergebnis der Verarbeitung durch KI entsprechend schlecht sein. Maßnahmen zur Wahrung der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Personen müssen bereits beim Training des Systems greifen. Diese vorbeugenden Maßnahmen sollten auch für die Datenschutzfolgenabschätzung dokumentiert werden. In der Praxis können die angemessenen Schutzmaßnahmen in einem vierstufigen Verfahren umgesetzt werden:[23]

1. Sicherstellung der diskriminierungsfreien Datenbasis: Trainingsdaten sowie das Verfahren des Maschinen E-Learning werden sorgfältig und repräsentativ ausgewählt und gepflegt, um

20 *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 25; *EDPS*, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit., 11.4.2017, S. 7.

21 *BGH* MMR 2017, 394, Rn. 70 – World of Warcraft II: „Der Erfolg eines solchen Spiels steht und fällt damit, dass für alle Spieler die gleichen Bedingungen für die Bewältigung der Aufgaben und das Erreichen höherer Levels gelten."

22 Vgl. auch Erwägungsgrund 71 S. 5.

23 Angelehnt an *Schulz* (o. Fußn. 12), Rn. 42.

eine „voreingenommen Datenbasis" („biased data") zu vermeiden. Datenherkunft und Erhebungskontext sollten dokumentiert sein.[24]

2. Information der betroffenen Personen: Die betroffenen Personen werden allgemein über die Tatsache der automatisierten Entscheidung informiert. Diese Information beinhaltet aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung (Art. 13, Art. 14 DS-GVO) und die Rechte nach Art. 20 Abs. 3 DS-GVO.[25] In diesem Zusammenhang sollte bevorzugt „Erklärbare Künstliche Intelligenz" („Explainable AI") zum Einsatz kommen.

3. Auskunft über Gründe der Ablehnung: Im Falle einer für die betroffene Person ungünstigen automatisierten Entscheidung, werden der betroffenen Person auf Anfrage die Gründe der Ablehnung mitgeteilt und erläutert, wie es Erwägungsgrund 71 vorsieht. Nur mit diesen Informationen ist die betroffene Person in der Lage, ihre weiteren Rechte nach Art. 22 Abs. 3 DS-GVO auszuüben.

4. Überprüfung und Korrektur der Entscheidung: Der Betroffene hat das Recht auf Remonstration der maschinellen Entscheidung und ein Eingreifen einer Person seitens des Verantwortlichen. Der eigene Standpunkt der betroffenen Person muss gehört und nötigenfalls die maschinelle Entscheidung korrigiert werden. Dazu sind den betroffenen Personen möglichst einfache Verfahren und Kommunikationszugänge zu dem Verantwortlichen bereitzustellen.

III. Zusammenfassung

Künstliche Intelligenz hat schon jetzt Ihren festen Platz im Ökosystem der Videospiele und wird in der Bedeutung für die Branche weiter steigen. Nicht alle Anwendungsgebiete der KI sind datenschutzrechtlich relevant, insbesondere aber bei automatisierten Entscheidungsfindungen sind die Anforderungen der DS-GVO relevant. Betrugsabwehr und Anti-Cheat-Verfahren basierend auf automatisierten Systemen wirken auf den ersten Blick wie Paradebeispiele für das grundsätzliche Verbot der ausschließlich maschinellen Entscheidungen über relevante Interessen der betroffenen Nutzer*innen. Bei genauerer Betrachtung spricht jedoch viel dafür, dass diese Maßnahmen in keinem unauflöslichen Konflikt mit Art. 22 DS-GVO stehen. Vielfach wird schon keine automatisierte Entscheidung vorliegen, weil es entweder schon an der echten Entscheidung fehlt oder diese im Wesentlichen von vornherein von einem oder mehreren Menschen determiniert ist. Weiter ist zweifelhaft, ob alle Anti-Cheat-Entscheidungen überhaupt beachtliche Auswirkungen für die betroffenen Personen haben. Nicht jede Bagatellentscheidung soll durch den würdeschützenden Art. 22 DS-GVO verboten werden. Zuletzt kann in einem effektiven Anti-Cheat-System – selbst wenn es sämtliche Verbotsmerkmale des Art. 22 Abs. 1 DS-GVO aufweist – ein für die Vertragsdurchführung erforderliche Datenverarbeitung liegen. In jedem Fall wird der Publisher angemessene Schutzmaßnahmen für den Einsatz der KI zur Entscheidungsfindung oder -vorbereitung treffen.

Schnell gelesen ...

- Bei automatisierten Entscheidungsfindungen in und um Videospiele sind die Anforderungen der DS-GVO relevant.
- Trifft die KI gänzlich automatisierte Entscheidungen, die für die betroffene natürliche Person von erheblicher Relevanz ist, erlaubt die DS-GVO dies nur in ganz engen Grenzen und Ausnahmefällen.
- Anti-Cheat-Verfahren basierend auf automatisierten Systemen wirken auf den ersten Blick wie Paradebeispiele für verbotene automatisierte Entscheidungen.
- Bei analysierender Betrachtung wird meist schon keine ausschließlich maschinelle Entscheidung vorliegen oder die Entscheidung ist vertraglich erforderlich.
- Publisher werden jedenfalls angemessene Schutzmaßnahmen für den Einsatz der KI zur Entscheidungsfindung oder -vorbereitung treffen.

Dr. Axel von Walter
ist Rechtsanwalt, Fachanwalt für Urheber- und Medienrecht, Fachanwalt für IT-Recht und Partner bei GvW Graf von Westphalen in München sowie Lehrbeauftragter an der LMU München für Medien- und Informationsrecht.

24 Vgl. dazu insgesamt *Art. 29-Datenschutzgruppe*, WP 251rev.01 v. 6.2.2018, S. 31 sowie Vorschläge für Maßnahmen S. 36 f.
25 Vgl. auch Fußn. 19.

FLEMMING MOOS

Durchsetzung der DS-GVO mittels Bußgeldern am Beispiel der Games-Branche

Was können Spieleunternehmen aus den bisherigen Bußgeldentscheidungen lernen?

Sanktionen

Dieser Beitrag analysiert die Praxis der Durchsetzung der DS-GVO mittels Bußgeldern in den ersten drei Jahren nach deren Wirksamwerden. Hierbei wird ein besonderer Fokus auf die Games-Branche gelegt. Neben einer Darstellung der Enforcement-Praxis werden in dem Beitrag auch die rechtlichen Problemfelder aufgezeigt und diskutiert, die sich bei der Verhängung von Bußgeldern wegen DS-GVO-Verstößen gegenüber Unternehmen ergeben. Lesedauer: 25 Minuten

I. Einleitung

Gut drei Jahre nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) lässt sich durchaus ein erstes Fazit dazu ziehen, ob und wie strikt die verschärften Datenschutzregeln in der Praxis tatsächlich auch angewendet und vor allem durchgesetzt werden. Die Panik war in vielen Unternehmen und teilweise ganzen Branchen groß vor dem Mai 2018. Vor allem Befürchtungen existenzvernichtender Millionenbußgeldern machten die Runde. Auch die Games-Branche wurde von der DS-GVO-Panik ergriffen.[1] Zudem machten Meldungen die Runde, nach denen sich einige Spieleanbieter vornehmlich US-amerikanischer Provenienz vom europäischen Markt zurückgezogen hätten, weil sie die DS-GVO-Anforderungen nicht (wirtschaftlich) hätten erfüllen können oder weil das Sanktionsrisiko unkalkulierbar sei. Mit der Möglichkeit, Bußgelder (bzw. im Sprachgebrauch der DS-GVO „Geldbußen") von bis zu 20 Mio. EUR bzw. bis zu 4% des weltweiten Jahresumsatzes zu verhängen, besitzen die Datenschutzbehörden durchaus ein sehr scharfes Schwert.

Und tatsächlich lässt sich feststellen, dass mittlerweile – häufig begleitet von ausführlicher Presseberichterstattung[2] – eine beträchtliche Zahl von Bußgeldern in durchaus erheblicher Höhe von europäischen Datenschutzaufsichtsbehörden verhängt worden sind. Millionenbußgelder, die gegenüber Internetkonzernen, Mode- und Immobilienunternehmen und TK-Dienstleistern verhängt worden sind, sind jedem gegenwärtig.[3] Just beim Finalisieren dieses Beitrag macht eine Meldung die Runde, wonach die *luxemburgische Datenschutzaufsichtsbehörde* beabsichtigt, *Amazon* mit einem Bußgeld i.H.v. 350 Mio. EUR zu belegen[4] – es wäre das bisher mit Abstand höchste Bußgeld wegen eines Datenschutzverstoßes. Doch sind diese Zahlen ein sinnvoller Gradmesser für andere Unternehmen – gerade auch für solche der Games-Branche?

1. Überblick über die Bußgeldpraxis

Ganz allgemein lässt die Bußgeldhöhe allein nur einen eingeschränkten Rückschluss auf die Strenge der Sanktionierung zu, weil sie von diversen Zumessungskriterien und – zu einem signifikanten Anteil – auch der Umsatzhöhe des betroffenen Unternehmens beeinflusst wird. Auch ein abstrakt eher gering erscheinender Betrag kann deshalb eine empfindliche Sanktion darstellen, weil z.B. das Unternehmen nur geringe Umsätze erwirtschaftete oder weil der sanktionierte Verstoß marginal war. Umgekehrt kann ein Millionenbußgeld für einen Konzern mit einem Milliardenumsatz dennoch eine vergleichsweise milde Sanktion darstellen. Insoweit sind allgemeine Ableitungen aus diesen Einzelfallentscheidungen generell schwierig.

Hinzu kommt, dass die Herangehensweise der Aufsichtsbehörden in den verschiedenen EU-Mitgliedstaaten durchaus voneinander abweicht: So existieren mehrere Mitgliedstaaten, in denen zwar durchaus eine rege Durchsetzungspraxis besteht, die Bußgeldhöhen aber bisher sehr moderat ausfallen (z.B. Ungarn mit einem bisherigen Maximalbußgeld von 288.000,– EUR, Belgien mit 600.000,– EUR oder aber auch die Niederlande mit 900.000,– EUR).

Neben der Höhe der Sanktionen ist für die Bemessung des Sanktionsrisikos naturgemäß auch die Kontrolldichte relevant. Auch hier besteht zwischen den einzelnen Mitgliedstaaten eine hohe Disparität: Eine besonders große Zahl von Bußgeldern sind bisher in Spanien und Deutschland (mit jeweils über 200), Italien, Rumänien und Ungarn verhängt worden. Aus den Mitgliedstaaten Irland, Kroatien, Portugal und – solange es noch zur EU gehörte – Großbritannien, hingegen sind jeweils im Verhältnis zu ihrer Größe nur sehr wenige Bußgelder bekannt geworden.

2. Games-Unternehmen als Bußgeldadressaten

Wenn man gleichwohl einmal versucht, aus den hunderten Bußgeldern, die in den letzten drei Jahren in der EU nach Maßgabe der DS-GVO verhängt worden sind, diejenigen herauszufiltern, bei denen konkret Games-Unternehmen betroffen waren, zeigt sich folgendes Bild: Bekannt geworden ist tatsächlich nur ein mit der Verhängung eins Bußgelds abgeschlossenes Bußgeldverfahren der *tschechischen Datenschutzaufsichtsbehörde*, in dem ein Betrag von sage und schreibe 980,– EUR gegen ein Spieleunternehmen festgesetzt wurde. Was war passiert? Bei einem Online-Rollenspiel konnten Unbefugte wegen mangelnder Sicherheitsvorkehrungen auf die Daten der registrierten Spieler*innen der Plattform zugreifen. Zunächst sah sich der Spielebetreiber mit einer erfolgreichen DDos-Attacke eines Angreifers konfrontiert. Der Spielebetreiber ergriff Maßnahmen zur Verbesserung der Sicherheit, dennoch waren weitere Hacking-Angriffe erfolgreich. Gegen Zahlung einer Geldsumme erklärte sich der Angreifer bereit, die Angriffe zu stoppen und dem Betreiber bei der Sicherung des Servers zu helfen. Der Spielebetreiber stimmte zu und der Angreifer stellte dem Betreiber eine Firewall zur Verfügung, die der Betreiber nach Überprüfung auf seinem Spieleservers installierte. Der Angreifer hatte sich jedoch heimlich eine Hintertür in den Quellcode eingebaut und erlangte hierüber Zugriff auf die Spielerdatenbank. Der Angreifer veröffentlichte die Spielerdatenbank und leitete die Website des Spiels auf seine Website um. Die Spielerdatenbank enthielt ungefähr 4.500 Accounts (Benutzername, Passwort in verschlüsselter Form, E-Mail-Adressen, IP-Adressen, Informationen zur Zahlung wie der aktuelle Zahlungsstatus, Anzahl der gekauften virtuellen Währung, Kontoinhaber, Zeitpunkt und Methode der Zahlung) und war für ungefähr 1,5 Stunden im Internet veröffentlicht. Der Betreiber unterbrach sofort den Betrieb des Spiel- und Datenbankservers, erstattete Strafanzeige und meldete den Verstoß den betroffenen Personen und der Datenschutzbehörde.[5]

Die *tschechische Datenschutzbehörde* sah darin einen Verstoß gegen Art. 5 Abs. 1 lit. f DS-GVO. Nach ihrer Auffassung hätte der Betreiber das System nicht von demjenigen „verbessern" lassen dürfen, der Urheber des DDoS-Angriffe war. Außerdem stellte die *Behörde* fest, dass der Spielebetreiber die Dienste von zwei Auftragsverarbeitern in Anspruch nahm, ohne Auftragsverarbeitungsverträge i.S.d. Art. 28 Abs. 2 DS-GVO geschlossen zu haben. Die *tschechische Datenschutzbehörde* verhängte ein Bußgeld von 25.000 CZK (entspricht ungefähr 980,– EUR). Weitere DS-GVO-Bußgelder gegen Games-Unternehmen sind bis dato nicht bekannt geworden. Allenfalls mag noch das Bußgeld gegen eine spanische Spielsalonkette erwähnenswert sein, die DS-GVO-widrig eine Videoüberwachungsanlage installiert hatte, welche auch die öffentliche Straße erfasste. Die *spanische Datenschutzaufsichtsbehörde* bewertete dies als einen Verstoß gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DS-GVO und beabsichtigte ein Bußgeld über 6.000,– EUR zu verhängen, das gegen sofortige Zahlung unter Rechtsmittelverzicht auf eine Summe von 3.600,– EUR gemindert wurde.[6]

---

1 Kennzeichnend hierfür z.B. der Artikel in der W&V im Mai 2018: Bedroht die DSGVO Video-Games wie League of Legends?; abrufbar unter: https://www.wuv.de/tech/bedroht_die_dsgvo_videogames_wie_league_of_legends.

2 S. hierzu: *Schefzig/Rothkegel/Cornelius*, in: Moos/Schefzig/Arning, Praxishdb. DSGVO, 2. Aufl. 2021, Kap. 16 Rn. 59 ff.

3 Einen guten Überblick über die durch europäische Aufsichtsbehörden verhängten Bußgelder bietet der „GDPR Enforcement Tracker", abrufbar unter: www.enforcementtracker.com.

4 Vgl. die Meldung auf heise.de v. 11.6.2021, abrufbar unter: https://www.heise.de/news/Datenschutz-Luxemburg-plant-350-Millionen-Euro-Strafe-fuer-Amazon-6068245.html.

5 Zu Einzelheiten s. https://www.uoou.cz/kontrola-zabezpeceni-osobnich-udaju-pri-provozovani-online-hry-fyzicka-osoba-podnikajici/ds-5723/archiv=0&p1=5653.

6 Entscheidung der *AEPD* v. 15.4.2019, abrufbar unter: https://www.aepd.es/es/documento/ps-00135-2019.pdf.

3. Verarbeitungsumstände bei Games-Unternehmen mit Sanktionspotenzial

Bedeutet dies nun aber wiederum, dass Games-Unternehmen sich zurücklehnen können, weil sie sich vermeintlich nicht im Fokus der Aufsichtsbehörden befinden? Das wäre sicherlich ebenfalls ein Trugschluss. Zum einen ist die Branchenzugehörigkeit an sich bereits kein wirklich relevantes Kriterium. Zwar kommt es durchaus vor, dass Datenschutzaufsichtsbehörden ihre proaktive Überwachungstätigkeit so strukturieren, dass sie Prüfungen gezielt in bestimmten Branchen vornehmen. Das ist aber eher die Ausnahme als die Regel. Zum anderen ist zu konstatieren, dass die Datenverarbeitungen von Games-Unternehmen[7] durchaus einige Merkmale aufweisen, die sie zu einer „gefahrgeneigten" Verarbeitung machen; etwa der häufig große Umfang der verarbeiteten Spielerdaten, die umfassenden Online-Tracking-Möglichkeiten oder auch manchmal die Jugendlichkeit der Spieler*innen, auf die sich die Daten beziehen. Ein relevanter Risikofaktor ist auch das Thema Datensicherheit. Gerade Online- oder Plattformspiele sind hier im Fokus. Dabei bleibt es häufig nicht bei so glimpflichen Auswirkungen wie in dem o.g. Fall des tschechischen Spieleanbieters: Nach Medienberichten soll der in der Szene unter dem Pseudonym *Gnosticplayers* bekannte Hacker unlängst von einem US-amerikanischen Spieleanbieter insgesamt ca. 200 Mio. Nutzerdaten erbeutet haben.[8] Gerade in letztgenannten Fällen einer Datenpanne gibt es häufig ein aufsichtsbehördliches „Nachspiel". Es gehört zum Standardvorgehen der Datenschutzaufsichtsbehörden, im Zuge der weiteren Untersuchungen der ihnen nach Art. 33 DS-GVO gemeldeten Datensicherheitsverletzungen zu prüfen, ob evtl. eigene Versäumnisse bei der Datensicherheit mitursächlich waren für das Abhandenkommen der Daten. Ist dies der Fall, drohen tatsächlich Bußgelder. Besonders prominent hat sich dies in den Fällen Marriott[9] und British Airways[10] gezeigt, aber auch bei deutschen Aufsichtsbehörden ist ein Sanktionsfokus im Bereich der Datensicherheit wegen fehlender technischer oder organisatorischer Maßnahmen erkennbar:[11]

- Nachdem es der Hackergruppe *Magecart* mit Hilfe von Skimming-Skripten gelungen war, innerhalb von zwei Wochen die persönlichen Daten und Zahlungsinformationen von 500.000 Kund*innen zu stehlen, verhängte die britische Datenschutzbehörde *ICO* gegen *British Airways* ein Bußgeld wegen unzureichender Sicherheitsmaßnahmen, weil diese den Hackerangriff erst möglich gemacht hatten.
- Im Fall Marriott hatten Hacker die Zahlungsinformationen und persönlichen Daten von 500 Mio. Kund*innen der Hotelkette kompromittiert. Die Infiltration des Unternehmensnetzwerks lag zwar schon vier Jahre zurück und erfolgt zudem noch zu einer Zeit, in der die betroffene Tochtergesellschaft noch gar nicht zur *Marriott*-Unternehmensgruppe gehörte, laut *ICO* habe *Marriott* es aber schuldhaft versäumt, i.R.e. Datenschutz-Due-Diligence beim Kauf der Gesellschaft die notwendigen Prüfungen vorzunehmen.

Als Zwischenfazit bleibt also, dass zwar in monetärer Hinsicht die Games-Branche von der Durchsetzung der DS-GVO mittels Bußgeldern bisher – soweit öffentlich bekannt – noch weitestgehend verschont geblieben ist. Ein allzu komfortables Ruhekissen ist dies aber leider nicht: Die Datenverarbeitung vieler Spieleunternehmen ist durchaus in mehrerlei Hinsicht risikogeneigt, sodass es nur eine Frage der Zeit sein dürfte, dass wir auch hier im Falle von Verstößen ein vermehrtes Enforcement erleben.

II. Aktuelle Problemfelder bei der Sanktionierung von Unternehmen

Es hat sich gezeigt, dass es für die Aufsichtsbehörden durchaus gar nicht so einfach ist, entsprechende Bußgeldbescheide in rechtskonformer Weise zu erlassen. Ein paar sehr aktuelle Stolpersteine im Zusammenhang mit der Bußgeldverhängung, die gegen die Rechtskonformität eines Bußgelds ins Feld geführt werden können, werden deshalb nachfolgend aufgezeigt.

1. Auswahl der Bußgeldschuldner

Auf rechtlich unsicheres Terrain begeben sich Aufsichtsbehörden zuweilen schon bei der Auswahl des Bußgeldschuldners. Von Gesetzes wegen richtet sich ein Bußgeld gem. Art. 83 Abs. 4, 5 und 6 DS-GVO gegen den Verantwortlichen für die jeweilige Datenverarbeitung, wobei auch Auftragsverarbeiter direkt mit einem Bußgeld belegt werden können.

a) Bußgeldverhängung bei mehreren Beteiligten

Hierbei hat – bei Beteiligung mehrerer – jeweils eine separate Sanktionierung je nach Verschuldensanteil zu erfolgen.[12] § 41 Abs. 1 S. 1 BDSG i.V.m. § 14 Abs. 1 S. 1 OWiG legt fest, dass bei einer Beteiligung von mehreren Handelnden (z.B. zwei gemeinsam Verantwortliche) beide ordnungswidrig handeln (und sie deshalb beide jeweils separat Adressat eines Bußgeldbescheids sein können).[13] Eine gesamtschuldnerische Haftung von mehreren Verantwortlichen oder zusammenarbeitenden Verantwortlichen und Auftragsverarbeitern sieht Art. 83 DS-GVO im Gegensatz zu Art. 82 Abs. 4 DS-GVO also nicht vor.

b) Bußgeldverhängung gegen verbundene Unternehmen

In der Praxis verhängen Aufsichtsbehörden Bußgelder teilweise allerdings auch gegen Unternehmen, denen selbst gar kein Datenschutzverstoß zur Last gelegt wird. So sind Fälle bekannt geworden, in denen ein Bußgeldbescheid (auch) gegenüber der Muttergesellschaft des Verantwortlichen erlassen wurde. Als Begründung verweisen die Aufsichtsbehörden hierbei auf den sog. kartellrechtlichen Unternehmensbegriff,[14] der hier auch i.R.d. DS-GVO anzulegen sei.[15] Danach ist ein Unternehmen jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung.[16] Entscheidendes Argument für eine entsprechende Anknüpfung im Datenschutzrecht ist die Verweisung in Erwägungsgrund 150 S. 3 DS-GVO auf Art. 101 und 102 AEUV. Diese bewirke, dass sich das Tatbestandsmerkmal „Unternehmen" in Art. 83 DS-GVO nicht auf das Rechtssubjekt, sondern funktional auf die wirtschaftliche Einheit beziehe.

---

7 S. hierzu ausf. der Beitrag von *Bänsch/Hentsch* in dieser Beilage.

8 Vgl. die Meldung auf golem.de v. 1.10.2019, abrufbar unter: https://www.golem.de/news/mobile-games-datenleck-bei-spielehersteller-zynga-1910-144188.html.

9 Vgl. die Meldung auf e-recht24.de v. 3.11.2020, abrufbar unter: https://www.e-recht24.de/news/datenschutz/12429-marriott-bussgeld-corona.html.

10 Vgl. die Meldung auf netzpolitik.org v. 9.7.2019, abrufbar unter: https://netzpolitik.org/2019/dsgvo-british-airways-soll-rekordstrafe-wegen-sicherheitsmaengeln-zahlen/.

11 Vgl. die Meldungen auf lto.de v. 11.11.2020, abrufbar unter: https://www.lto.de/recht/nachrichten/n/lg-bonn-29owi120lg-bussgeld-1und1-datenschutzverstoss-dsgvo-millionen-herabgesetzt/ und auf heise.de v. 22.11.2018, abrufbar unter: https://www.heise.de/newsticker/meldung/Passwoerter-im-Klartext-20-000-Euro-Bussgeld-nach-DSGVO-gegen-Knuddels-de-4229798.html.

12 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 8 Rn. 36.

13 *Moos/Rothkegel*, in: Moos, Datenschutz und Datennutzung, 3. Aufl. 2021, § 5 Rn. 118.

14 Zum kartellrechtlichen Unternehmensbegriff s. *EuGH* U. v. 16.3.2004 – C-264/01, C-306/01, C-354/01, C-355/01, Rn. 46 – AOK Bundesverband u.a./Ichthyol-Gesellschaft Cordes, Hermani & Co. u.a.; s.a. *Bergt*, in: Kühling/Buchner, DS-GVO BDSG, Art. 83 Rn. 40 mwN.

15 *LG Bonn* ZD 2021, 154 (157) m. Anm. *von dem Bussche; Ebner/Schmidt*, CCZ 2020, 84; *Golla*, in: Auernhammer, DSGVO BDSG, Art. 83 Rn. 25 f.; *Holländer*, in: Wolff/Brink, BeckOK DatenschutzR, 36. Ed., Art. 83 Rn. 14.1; *Albrecht/Jotzo*, (o. Fußn. 12), Rn. 35; *Hohmann*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2016, § 3 Rn. 321; *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, S. 134; *Dieterich*, ZD 2016, 260 (265); *Neuhöfer/Schmidt*, jurisPR-Compl 3/2017 Anm. 5; *Rost*, RDV 2017, 13 (16 f.); *Schönefeld/Thomé*, PinG 2017, 126 (127).

16 *EuGH* U. v. 11.7.2006 – C-205/03 P, Rn. 25 – FENIN mwN.; ausf. zum weiten Verständnis der *EU-Kommission* und des *EuGH Cornelius*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl., Teil XIV Rn. 90 ff.

Schon diese Ausgangsthese ist freilich äußerst umstritten und es bestehen sehr gute Gegenargumente. So wird maßgeblich entgegnet, dass Erwägungsgrund 150 nicht die eigentlichen Normen der DS-GVO überschreiben dürfe, weshalb auf die Definition des Art. 4 Nr. 18 DS-GVO zurückzugreifen und somit ein Unternehmen gerade nicht einer Unternehmensgruppe (Art. 4 Nr. 19 DS-GVO) gleichzustellen sei.[17] Dieser Argumentationsansatz wird vom *EuGH* gestützt, wonach Widersprüche zwischen dem Wortlaut von Erwägungsgründen und dem eigentlich Rechtstext aufzulösen sind.[18] Auch der Sache nach erscheint es aber bedenklich, ein Unternehmen allein auf Grund des Bestehens einer gesellschaftsrechtlichen Verbindung mit dem Delinquenten als Haftungssubjekt auszuerkiesen. Der Wortlaut von Art. 83 Abs. 2 und 3 DS-GVO bestimmt, dass nur Verantwortliche und Auftragsverarbeiter bußgeldbewerte Verstöße begehen können – und folglich auch nur selbst Adressat eines Bußgelds sein können.[19] Aus Art. 83 Abs. 4, 5 und 6 DS-GVO und Erwägungsgrund 150 ergibt sich nichts anderes, denn diese Vorschriften regeln nur die Höhe des Bußgelds,[20] sie dehnen aber nicht die Gruppe der möglichen Bußgeldadressaten aus. Eine andere Auslegung erscheint unvereinbar mit dem Grundsatz „nulla poena sine lege".[21]

Eine Parallele zum Kartellrecht verbietet sich, weil sich die Rechtslage nach der DS-GVO unterscheidet: Im Unterschied zum Kartellverbot richten sich die DS-GVO-Regeln gerade nicht abstrakt an „Unternehmen", sondern an Verantwortliche und Auftragsverarbeiter. Im Datenschutzrecht ist im Gegensatz zum Kartellrecht deshalb gerade kein Funktionsträgerprinzip, sondern ein Rechtsträgerprinzip verankert.[22] Weil aber richtigerweise keine Trennung zwischen Verstoß (Tatbestandsseite) und dem materiell-rechtlichen Haftungsadressaten (Rechtsfolgenseite) stattfindet, kann die Bußgeldhaftung eben nur dem Rechtssubjekt auferlegt werden, welches den Verstoß auch begangen hat.[23] Die Einbeziehung z.B. der Muttergesellschaft des verstoßenden Unternehmens in den Bußgeldbescheid ist deshalb nur möglich, wenn diese eine datenschutzrechtliche Bußgeldverantwortung trifft – etwa als Auftragsverarbeiter oder als gemeinsam Verantwortliche.[24] Nur die Eigenschaft als verbundenes Unternehmen rechtfertigt aber nicht den Erlass eines Bußgeldbescheids gegen die Muttergesellschaft.

2. Voraussetzungen für die Verhängung eines Bußgelds gegen ein Unternehmen

Nicht minder wackelig ist häufig die Begründung der Aufsichtsbehörde dafür, dass überhaupt ein Unternehmen – also im Regelfall eine juristische Person – mit einem Bußgeld belegt wird. Dem deutschen Recht (jenseits des Kartellrechts) ist der in der DS-GVO verankerte Ansatz, dass eine juristische Person als Unternehmen i.S.d. Art. 83 DS-GVO selbst Adressatin eines Bußgelds sein kann, grundsätzlich fremd. Im deutschen Recht gibt es deshalb die Zurechnungsnormen im OWiG, insbesondere § 30 OWiG, die die notwendigen Voraussetzungen dafür enthalten, dass eine juristische Person bebußt werden darf.

Die Behörden stehen bisher auf dem Standpunkt, dass sich aus Art. 83 DS-GVO eine unmittelbare Verbandshaftung des Unternehmens ergebe und wegen des Anwendungsvorrangs der DS-GVO die Regelungen in §§ 30, 130 OWiG nicht anwendbar seien.[25] Auf Grund dieser Positionierung unterlassen sie es in ihren Bußgeldbescheiden häufig, gem. § 30 Abs. 4 OWiG das Organmitglied oder die Leitungsperson zu bestimmen, deren schuldhaftes Handeln dem Unternehmen zugerechnet werden soll.

Es ist derzeit allerdings höchst umstritten, ob diese zusätzlichen Anforderungen nach §§ 30, 130 OWiG von der DS-GVO verdrängt werden,[26] oder ob sie auch im Falle von Bußgeldern nach Art. 83 DS-GVO weiter anwendbar sind mit der Folge, dass die Aufsichtsbehörde eine hinreichende Anknüpfungstat ermitteln müsste.[27] Es lässt sich durchaus – entgegen der weit verbreiteten Behördenpraxis – sehr gut vertreten, dass die §§ 30, 130 OWiG auch i.R.v. Art. 83 DS-GVO anzuwenden sind.[28] Nach § 41 Abs. 1 S. 1 BDSG gelten für Verstöße gem. Art. 83 Abs. 4 bis 6 DS-GVO die Vorschriften des OWiG sinngemäß, soweit das BDSG nichts anderes bestimmt. Von der Anwendbarkeit auf datenschutzrechtliche Verstöße sind gem. § 41 Abs. 1 S. 2 BDSG nur die §§ 17, 35 und 36 OWiG ausgenommen. §§ 30, 130 OWiG werden jedoch nicht erwähnt.

Die Auffassung kann sich zudem auf die Gesetzesmaterialien zum BDSG stützen, wonach es sich um eine bewusste Entscheidung des deutschen Gesetzgebers gehandelt hat, weil er der Anregung der *DSK*, §§ 30, 130 OWiG in § 41 BDSG von der Anwendung auf datenschutzrechtliche Ordnungswidrigkeitsverfahren auszunehmen, gerade nicht gefolgt ist. Es ist auch zu berücksichtigen, dass das gemeinschaftsrechtliche Sanktionsrecht insgesamt eher noch fragmentarischen Charakter besitzt. Gerade in diesem grundrechtssensiblen Bereich bedarf es aber klarer verfahrensmäßiger Festlegungen. Dies gilt umsomehr angesichts der enormen Höhe der nach Art. 83 DS-GVO möglichen Bußgelder – vor allem in der Auslegung der Aufsichtsbehörden, die bei der Bußgeldzumessung (wie gezeigt) auf den kartellrechtlichen Unternehmensbegriff abstellen. Hinreichende verfahrensrechtliche Festlegungen enthält hier aber nur das OWiG, sodass auf dessen Anwendbarkeit im Verfahren nach Art. 83 DS-GVO nicht verzichtet werden kann.

Die Regelungen in §§ 30, 130 OWiG werden deshalb nicht durch einen Vorrang des Europarechts verdrängt, sie lassen sich auf die Öffnungsklausel in Art. 83 Abs. 8 DS-GVO stützen.[29] Hierüber überlässt die DS-GVO dem nationalen Gesetzgeber u.a. Regelungen zur Zurechnung eines Verstoßes zu einem Unternehmen selbst zu treffen.[30]

Richtigerweise muss in einem Bußgeldbescheid deshalb nicht nur der Tatvorwurf hinreichend konkretisiert sein, es muss nach § 30 Abs. 4 OWiG das Organmitglied oder die Leitungsperson bestimmt sein, deren schuldhaftes Handeln dem Unternehmen zugerechnet werden soll. Genügt ein Bußgeldbescheid diesen Anforderungen nicht, sollten Rechtsmittel geprüft werden.

---

17 *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, Art. 83 Rn. 20; *Faust/Spittka/Wybitul*, ZD 2016, 120 (123 ff.); *Feldmann*, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2017, Art. 83 Rn. 30; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 1121; *Piltz*, K&R 2017, 85 (92), auch für die englische Fassung der DS-GVO; *Grünwald/Hackl*, ZD 2017, 556 (558 f.); *Grünwald/van der Wolk/Hackl*, Privacy & Security Law Report, 16 PVLR 1359, 10/9/17, S. 3.

18 *EuGH* U. v. 19.6.2014 – C-345/13 – Karen Millen Fashions; *EuGH* U. v. 24.11.2005 – C-136/04 – Deutsches Milchkontor; *EuGH* U. v. 25.11.1998 – C-308/97 – Manfredi; *EuGH* U. v. 19.11.1998 – C-162/97 – Nilsson.

19 *Ebner/Schmidt*, CCZ 2020, 84 (85).

20 *LG Berlin* ZD 2021, 270 m. Anm. *von dem Bussche*, Rn. 24.

21 *LG Berlin* ZD 2021, 270 m. Anm. *von dem Bussche*, Rn. 23; hierzu: *Kühn/Sembritzki*, ZD 2021, 193 (194).

22 A.A. *Ambrock*, ZD 2020, 492 (493).

23 *Adelberg/Spittka/Zapf,* CB 2021, 149 (152); a.A. wohl: *Holländer* (o. Fußn. 15), Rn. 10 ff.

24 Hierzu *Ebner/Schmidt*, CCZ 2020, 84 (85 ff.).

25 *LG Bonn* ZD 2021, 154 m. Anm. *von dem Bussche*; *Bergt* (o. Fußn. 14), Rn. 20; *Ambrock*, ZD 2020, 492 (496).

26 *LG Bonn* ZD 2021, 154 (155) m. Anm. *von dem Bussche*.

27 Einen guten Überblick über den Streitstand bieten: *Adelberg/Spittka/Zapf,* CB 2021, 149 (151).

28 *LG Berlin* ZD 2021, 270 m. Anm. *von dem Bussche*, Rn. 11, 16; *Popp*, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 83 Rn. 5; *Gola*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83 Rn. 11; *Schantz/Wolff* (o. Fußn. 17), Rn. 1128; *Taeger/Spittka*, DSB 2020, 292 (293).

29 *LG Berlin* ZD 2021, 270 m. Anm. *von dem Bussche*, Rn. 16; a.A. *Ambrock*, ZD 2020, 492 (496).

30 *Messner*, ZD 2020, 463 (466); *Popp* (o. Fußn. 28); *Gola* (o. Fußn. 28), Rn. 11, 16 f.; *Venn/Wybitul*, NStZ 2021, 204 (209); zu der insoweit vergleichbaren Rechtslage in Österreich: *ÖVGH* ZD 2020, 463 m. Anm. *Messner*.

3. Höhe des Bußgelds

Schließlich besteht eine erhebliche Unsicherheit auch bei der Frage, in welcher Höhe ein Bußgeld angemessen und rechtmäßig ist. Ausgangspunkt hierfür ist Art. 83 Abs. 2 DS-GVO, der gesetzlich Zumessungskriterien für Bußgelder normiert. Ist die Entscheidung über das „Ob" der Verhängung eines Bußgelds gefallen, besteht unter dem Bußgeldrahmen des Art. 83 Abs. 4 bis 6 DS-GVO aber ein großer Spielraum für das Ermessen der Aufsichtsbehörden über die Höhe des Bußgelds (Auswahlermessen).[31] Mit dem Ziel, die Behördenpraxis der Bußgeldzumessung in Deutschland etwas zu vereinheitlichen und zu standardisieren, haben die in der *DSK* zusammengeschlossenen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 14.10.2020 ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen beschlossen.[32] Das Konzept bindet nur die deutschen Aufsichtsbehörden und gilt insbesondere nicht für grenzüberschreitende Fälle. Es findet nur auf Unternehmen Anwendung, nicht aber z.B. auf Vereine oder natürliche Personen außerhalb einer wirtschaftlichen Tätigkeit. Es ist hierbei sehr umstritten, ob das *DSK*-Bußgeldmodell mit den gesetzlichen Zumessungsvorschriften in Art. 83 Abs. 2 DS-GVO wirklich vereinbar ist – in seinem Urteil zum Bußgeldbescheid gegen *1&1* hat das *LG Bonn* die auf Basis dieses Konzepts ermittelte Bußgeldhöhe für unverhältnismäßig erachtet.

a) Kriterien für die Bußgeldzumessung

Nach dem *DSK*-Konzept erfolgt die Bußgeldzumessung in Verfahren gegen Unternehmen in fünf Schritten:

- (1) Zunächst wird das Unternehmen einer Größenklasse zugeordnet: Die Größenklassen richten sich nach dem gesamten, weltweit erzielten Vorjahresumsatz des Unternehmens. Es erfolgt hierbei eine Einteilung in kleine, mittlere und Großunternehmen, die sich an der Empfehlung der *Kommission* v. 6.5.2003[33] orientiert.
- (2) Danach erfolgt die Bestimmung des mittleren Jahresumsatzes für die jeweilige Größenklasse: Ab einem jährlichen Umsatz von über 500 Mio. EUR ist der prozentuale Bußgeldrahmen von 2% bzw. 4% des jährlichen Umsatzes als Höchstgrenze zu Grunde zu legen, sodass beim jeweiligen Unternehmen eine Berechnung anhand des konkreten Umsatzes erfolgt.
- (3) Anschließend ermittelt die Aufsichtsbehörde den sog. wirtschaftlichen Grundwert (entspricht einem „Tagessatz"): Hierfür wird der mittlere Jahresumsatz der relevanten Größenklasse, in die das Unternehmen eingeordnet wurde, durch 360 (Tage) geteilt und so ein durchschnittlicher, auf die Vorkommastelle aufgerundeter Tagessatz errechnet.
- (4) Im nächsten Schritt wird dieser Grundwert mit einem von der Schwere der Tat abhängigen Faktor multipliziert: Hierbei nehmen die Aufsichtsbehörden anhand der konkreten tatbezogenen Umstände des Einzelfalls i.S.v. Art. 83 Abs. 2 S. 2 DS-GVO eine Einordnung des Schweregrads der Tat in leicht, mittel, schwer oder sehr schwer vor. Je nachdem, ob es sich dabei um formelle (Art. 83 Abs. 4 DS-GVO) oder materielle (Art. 83 Abs. 5, 6 DS-GVO) Verstöße handelt, gelten jeweils unterschiedliche hohe Faktoren.
- (5) Im letzten Schritt nehmen die Behörden noch eine Korrektur des Werts anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände vor: Es erfolgt nochmals eine Gesamtabwägung unter Berücksichtigung aller für und gegen das Unternehmen sprechenden Umstände, soweit diese noch nicht unter (4) berücksichtigt wurden. Neben den Kriterien nach Art. 83 Abs. 2 DS-GVO sollen hier auch Umstände eine Rolle spielen wie eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens.

b) Schlussfolgerungen aus der Anwendung des Bußgeldkonzepts in der Praxis

Mittlerweile ist das *DSK*-Bußgeldkonzept schon in mehreren Verfahren angewendet worden, sodass gewisse Praxiserfahrungen bereits bestehen. Hierbei ist aber bisher noch nicht ausreichend transparent, ob die Aufsichtsbehörden die verabredeten Kriterien auch in gleicher Weise anwenden. Dies ist misslich, weil entscheidende Aspekte offen bleiben; z.B. die Gewichtung der Zumessungskriterien untereinander.[34] Folgende erste Schlüsse lassen sich aus den bisherigen Anwendungsfällen ziehen:

Umsatzzentrierter Berechnungsansatz

Für den Fall, dass ein DS-GVO-Verstoß durch ein Unternehmen begangen wird, bestimmt sich der Bußgeldrahmen gem. Art. 83 Abs. 4, 5 und 6 DS-GVO grundsätzlich nach der Höhe seines „gesamten, weltweit erzielten Jahresumsatzes". Die *DSK* macht den Unternehmensumsatz in ihrem Bußgeld-Konzept hierbei sogar zum Dreh- und Angelpunkt der Bußgeldberechnung, was aus sich heraus unter dem Gesichtspunkt der Verhältnismäßigkeit rechtlich bereits fragwürdig ist.[35] Der Umsatz ist als Zumessungsgesichtspunkt in Art. 83 Abs. 2 S. 2 DS-GVO gar nicht genannt. Aber auch in wirtschaftlicher Hinsicht ist die Methode nicht ausgereift: Eine primär umsatzbezogene Bußgeldzumessung führt regelmäßig dazu, dass ein Bußgeld selbst für einen geringen Verstoß eines umsatzstarken Unternehmens leicht eine Millionenhöhe erreichen kann, während selbst sehr schwerwiegende Verstöße umsatzschwacher Unternehmen mit Minimalbeträgen sanktioniert würden.[36] In solchen Fällen führt diese Umsatzzentrierung nicht mehr zu angemessenen Ergebnissen. Dies hat auch das *LG Bonn* bereits ausdrücklich so entschieden und deshalb das vom *BfDI* gegen *1&1* verhängte Bußgeld von einem Betrag von 9,55 Mio. EUR auf 900.000,– EUR herabgesetzt.

Bußgelder auf Grundlage des *DSK*-Bußgeldmodells sind deshalb ggf. strukturell zu hoch. Allein aus diesem Grund mag ein Rechtsmittel gegen einen Bußgeldbescheid sinnvoll sein, wobei hierbei die Umstände des Einzelfalls zu berücksichtigen sind.

Begrenzung des relevanten Umsatzes

Die Behörden haben deshalb ein Eigeninteresse daran, das Bußgeldmodell so anzuwenden, dass es den Anforderungen des Verhältnismäßigkeitsprinzips genügt. Um durch eine pauschale Bezugnahme auf den weltweiten Jahresumsatzes nicht aus dem Rahmen zu fallen, kommt es vor, dass Aufsichtsbehörden bei der Berechnung des für den Verstoß anzuwenden Tagessatzes gemäß Schritt (3) des Konzepts nicht notwendigerweise auf den weltweiten Umsatz abstellen; abhängig vom Verstoß kann auch eine regionale oder gegenständliche Begrenzung des relevanten Umsatzes erfolgen. Dieser Vorgehensweise ist zuzustimmen; sie ist rechtlich sogar geboten: Selbst wenn man – wie es die *DSK* in ihrem Konzept vertritt – bei der Festsetzung des relevanten Unternehmensumsatzes auf den kartellrechtlichen Unternehmensbegriff gem. Art. 101, 102 AEUV abstellen wollte, müsste man sich jedenfalls i.Ü. auch an denjenigen Maßstäben für die Berechnung des Umsatzes orientieren, die im Rahmen eben dieser kartellrechtlichen Betrachtung nach Art. 101 und 102 AEUV von der *EU-Kommission* und dem *EuGH* angewendet werden. Diese ergeben sich für die Verhängung von Bußgeldern auf Grund von Verstößen gegen Art. 101 und 102 AEUV aus den

31 *Holländer* (o. Fußn. 15), Rn. 27.
32 Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen v. 14.10.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf.
33 Empfehlung der *Kommission* v. 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl. Nr. L 124 v. 20.5.2003, S. 36.
34 *Lang*, CB 2020, 20 (22).
35 Als „problematisch" eingestuft von: *LG Bonn* ZD 2021, 154 (158) m. Anm. *von dem Bussche*; krit. auch: *Lang*, CB 2020, 20 (22).
36 *Behr/Tannen*, CCZ 2020, 120 (124).

Leitlinien für das Verfahren zur Festsetzung von Geldbußen gem. Art. 23 Abs. 2 lit. a der Verordnung Nr. 1/2003 (im Folgenden: Leitlinien).

Die Anwendung dieser Leitlinien ist insbesondere auch vom *EuGH* zur Bestimmung des relevanten Umsatzes abgesegnet. Nach st. Rspr. des *EuGH* zielt Ziff. 13 der Leitlinien darauf ab, bei der Berechnung der Höhe der gegen ein Unternehmen verhängten Geldbuße einen Betrag als Ausgangspunkt festzulegen, der die wirtschaftliche Bedeutung der Zuwiderhandlung und das jeweilige Gewicht dieses Unternehmens daran wiedergibt. Folglich könne der in Ziff. 13 der Leitlinien von 2006 verwendete Umsatzbegriff nicht so weit ausgedehnt werden, dass er die von dem betreffenden Unternehmen getätigten Verkäufe umfasst, die nicht von dem zur Last gelegten Kartell erfasst werden.[37]

Auf Verstöße gegen die DS-GVO übertragen lässt sich hieraus schlussfolgern, dass auch der für ein DS-GVO-Bußgeld zu bildende Grundbetrag nur denjenigen Teil des Umsatzes darstellen darf, der von dem zur Last gelegten Verstoß „erfasst ist". Die analoge Anwendung der *Kommissions*-Leitlinien ist hier auch deshalb besonders naheliegend, weil sie – im Gleichlauf mit dem Konzept der *DSK* zur Bußgeldbemessung – zunächst die Ermittlung eines Grundbetrags vorsieht, der dann anschließend – je nach Schwere des Verstoßes nach oben oder unten angepasst wird (vgl. Ziff. 10 und 11 der Leitlinien).

Nach Ziff. 9 ff. dieser Leitlinien bestimmt sich der relevante Grundbetrag (entsprechend dem Referenzwert nach dem *DSK*-Bußgeldmodell) dabei nach dem Wert der von dem betreffenden Unternehmen im relevanten räumlichen Markt innerhalb des EWR verkauften Waren oder Dienstleistungen, die mit dem Verstoß in einem unmittelbaren oder mittelbaren Zusammenhang stehen (vgl. Leitlinien, Ziff. 13). Das bedeutet, der Umsatz ist sowohl in räumlicher als auch in sachlicher Hinsicht zu begrenzen, um den Grundbetrag zu bestimmen: In räumlicher Hinsicht ist dabei festzustellen, auf welchem (geografischen) Markt sich ein Verstoß auswirkt. Nur die auch dort erzielten Umsätze dürften berücksichtigt werden. Zudem ist der relevante Umsatz auch sachlich zu bestimmen; z.B. danach, auf welches Produkt oder Leistungsangebot oder welche Personengruppe sich der Verstoß bezieht. Bei der Multiplikation des Grundwerts in Schritt (4) orientieren sich die Aufsichtsbehören augenscheinlich vorwiegend an dem Faktor gem. Art. 83 Abs. 2 lit. a DS-GVO. Hierbei nehmen sie teilweise eine gesonderte Bewertung in qualitativer und in quantitativer Hinsicht vor. Qualitative Kriterien sind u.a. die Art der personenbezogenen Daten und die Art der Verarbeitung, quantitative insbesondere die Anzahl der betroffenen Personen und der Datensätze. Sofern bei diesen beiden Bewertungsdimensionen unterschiedliche Faktoren herauskommen, wird sodann ein Mittelwert gebildet. Bei der Anpassung des Grundwerts anhand aller sonstigen für und gegen den Betroffenen sprechenden Umstände gemäß Schritt (5) berücksichtigen die Aufsichtsbehörden vor allem die übrigen Zumessungskriterien nach Art. 83 Abs. 2 lit. b bis lit. k DS-GVO. Erste Praxiserfahrungen zeigen, dass die Gewichtung dieser Kriterien sehr stark einzelfallabhängig ist. Ein paar allgemeine Rückschlüsse lassen sich dennoch ziehen:

- Maßnahmen zur Minderung der Auswirkungen und zur Abstellung eines Verstoßes sowie eine gute proaktive Kooperation mit der Aufsichtsbehörde können sich stark bußgeldmindernd auswirken;
- Der Umstand, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, besitzt eine hervorgehobene Bedeutung und geht stärker in die Wertung ein als andere Kriterien;
- Auch Reputationsschäden auf Grund des Datenschutzverstoßes (bzw. maßgeblich der Berichterstattung hierüber) können Berücksichtigung finden;
- Wichtig ist, dass auch eine mit der Aufsichtsbehörde gefundene Verständigung wegen der damit zum Ausdruck gebrachten Einsicht in den Unrechtsgehalt eine substanziell bußgeldmindernde Wirkung haben kann.

Ob diese Versuche einer Abmilderung der Umsatzrelevanz das Bußgeldmodell retten, ist offen. In der Literatur wird der Fortbestand des Modells kritisch gesehen.[38] Wie bereits dargestellt, hat das *LG Bonn* die primär umsatzbezogene Bußgeldberechnung, wie sie das aktuelle *DSK*-Bußgeldkonzept festlegt, für unverhältnismäßig erachtet.[39] Ob und wann eine Anpassung des *DSK*-Bußgeldmodells erfolgt, steht jedoch noch nicht fest.

III. Fazit

Bisher sind Unternehmen der Games-Branche soweit ersichtlich noch von großen DS-GVO-Bußgeldern verschont geblieben. Aber das muss nicht auf ewig so weitergehen: Weil die Datenverarbeitungen vieler Games-Unternehmen gewisses Gefährdungspotenzial birgt, kann ein relevanter DS-GVO-Verstoß durchaus ein empfindliches Bußgeld nach sich ziehen. Mit dem Erhalt eines solchen Bußgeldbescheids ist aber nicht notwendigerweise die letzte Messe gelesen: Die behördliche und vor allem auch schon die gerichtliche Praxis zu DS-GVO-Bußgeldverfahren zeigt, dass die Bescheide nicht selten mangelhaft sind. Es sollte deshalb genau geprüft werden, ob und wenn ja, welche Defizite ein Bußgeldbescheid enthält und ob deshalb ein Rechtsmittel ergriffen werden soll.

Schnell gelesen ...

- Gegen Games-Unternehmen sind bisher – soweit bekannt – noch keine gravierenden Bußgelder wegen DS-GVO-Verstößen verhängt worden
- Die Datenverarbeitungen vieler Games-Unternehmen weisen aber durchaus ein signifikantes Risikopotenzial auf, u.a. wegen der Menge an Daten, der Sicherheitbedrohungen im Online-Bereich (Cybersecurity) und teilweise auch der Jugendlichkeit der Spieler*innen.
- DS-GVO-Verstöße und Bußgelder als Sanktionen sind deshalb durchaus im Bereich des Möglichen.
- Die Praxis zeigt, dass viele Rechtsfragen rund um die rechtmäßige Verhängung von Bußgeldbescheiden gegenüber Unternehmen wegen DS-GVO-Verstößen unklar und umstritten sind.
- Auch das DSK-Modell für die Zumessung von Bußgeldern selbst erscheint nicht durchgängig mit den DS-GVO-Anforderungen vereinbar.
- Im Fall der Fälle empfiehlt sich deshalb eine sorgsame Prüfung von Rechtsmitteln gegen einen Bußgeldbescheid.

Dr. Flemming Moos
ist Rechtsanwalt und Partner bei Osborne Clarke in Hamburg.

37 *EuGH* U. v. 11.7.2013 – C-444/11 P, Rn. 76 – Team Relocations u.a./Kommission, nicht veröffentlicht (EU:C:2013:464); U. v. 12.11.2014 – C-580/12 P, Rn. 57 – Guardian Industries und Guardian Europe/Kommission (EU:C:2014:2363); U. v. 19.3.2015 – C-286/13 P, Rn. 148 – Dole Food und Dole Fresh Fruit Europe/Kommission (EU:C:2015:184); U. v. 23.4.2015 – C-227/14 P, Rn. 53 – LG Display und LG Display Taiwan/Kommission (EU:C:2015:258) und U. v. 7.9.2016 – C-101/15 P, Rn. 19 – Pilkington Group u.a./Kommission (EU:C:2016:631).

38 *Adelberg/Spittka/Zapf,* CB 2021, 149 (152); *Taeger/Spittka*, DSB 2020, 292 (293).

39 *LG Bonn* ZD 2021, 154 (158) m. Anm. *von dem Bussche*; krit. auch: *Lang*, CB 2020, 20 (22).

Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!

IHR GESCHENK

SONDERAUSGABE DER AUSKUNFTS-ANSPRUCH NACH ART. 15 DS-GVO

Die große Zeitschrift zum Datenschutz

Die ZD informiert umfassend über die relevanten datenschutzrechtlichen Aspekte aus allen Rechtsgebieten und begleitet die nationale sowie internationale Gesetzgebung und Diskussion um den Datenschutz. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B. ‣ Konzerndatenschutz ‣ Beschäftigtendatenschutz ‣ Datenschutz-Folgenabschätzung ‣ Compliance ‣ Kundendatenschutz ‣ Telekommunikation ‣ Soziale Netzwerke ‣ Datentransfer in Drittstaaten ‣ Vorratsdatenspeicherung ‣ Informationsfreiheit ‣ Profiling und Scoring ‣ Tracking.

Geschaffen für die Unternehmenspraxis

Jedes Heft enthält ein Editorial, Aufsätze mit Lösungsvorschlägen, Angaben zur Lesedauer, Abstracts in Deutsch und Englisch, Schlagwortketten, Entscheidungen mit Anmerkungen und aktuelle Meldungen.

Alles inklusive:

- Online-Modul ZDDirekt – vollständiges Online-Archiv ab ZD 1/2011
- 14-täglicher Newsdienst ZD-Aktuell
- Homepage www.zd-beck.de
- Fundstellen-Recherche in beckonline.

3 Hefte gratis

Bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/go/ZD.

ZD – Zeitschrift für Datenschutz

11. Jahrgang. 2021. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 279,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS
sowie für ausgewählte Kooperationspartner € 219,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 15,– jährlich.

beck-shop.de/go/ZD

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK