Bundesministerium
für Bildung
und Forschung

DOS

Datenschutz in Online-Spielen

Studie im Auftrag des BMBF

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Studie

– Datenschutz in Online-Spielen –

Projektnummer: 16I1578

Studie im Auftrag des
Bundesministeriums für Bildung und Forschung

Verfasser:

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, 24103 Kiel
http://www.datenschutzzentrum.de/

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

September 2010

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Executive Summary

Aktuelle Situation

Online-Spiele erfreuen sich wachsender Beliebtheit. Betreiber aus aller Welt bieten die Spiele auf ihren unterschiedlichen Plattformen an. Waren es zunächst vor allem die PCs mit ihren Online-Rollenspielen und Browsergames, die den Trend gesetzt haben, so ist heute in den aktuellen Spielkonsolen die Online-Funktionalität eines der größten Verkaufsargumente. Doch auch Handys, wie das iPhone, oder zahlreiche andere Handheld-Geräte erlauben inzwischen das Spielen allein oder gemeinsam mit anderen Spielern von allen Orten, an denen ein (Mobilfunk-)Netz vorhanden ist. Online-Spiele erlauben die Verwaltung von Spieler-Freunden, die Kommunikation mittels Text, Sprache und Bild sowie die Integration von Sozialen Netzwerken wie Facebook und Twitter. Im Gegenzug wächst rasant die Zahl der Spiele, die direkt in Sozialen Netzwerken wie Facebook oder StudiVZ gespielt werden.

Das Problem

Online-Spiele benötigen Informationen über die Menschen, die sie nutzen. Dies sind Angaben für die Vertragsgestaltung und die Bezahlung, aber auch Daten über das Nutzungsverhalten des einzelnen Spielers. Die Erfassung einiger dieser Informationen ist für den Spieler erkennbar, etwa wenn er ein Formular ausfüllen muss. Andere Daten jedoch werden ohne sein Zutun oder sein bewusstes Einverständnis erhoben und verwendet. Mit dem Ziel, Raubkopierer und Schummler zu bekämpfen, werden etwa bei einigen Spielen im Hintergrund Informationen über den Computer und über die darauf vorhandenen Dateien und Programme erfasst – Daten, die auch viel über den Nutzer des Rechners aussagen können.

Auch Informationen darüber, welche Spiele wann und wie gut gespielt werden, werden verarbeitet und teilweise sogar frei abrufbar ins Web gestellt. Nicht nur Werbetreibende können hieran Interesse haben, sondern auch etwa (potentielle) Arbeitgeber und Kollegen. Eine Gefahr besteht insbesondere dann, wenn die öffentlichen oder auch geheimen bzw. internen Informationen mit weiteren Daten in Verbindung gebracht werden. Ist jemand etwa in der Lage, über Soziale Netzwerke, Suchmaschinen oder auch persönliche Kontakte ein umfassendes Profil über den Spieler zu erstellen, dann ergeben sich hieraus Vermutungen und Rückschlüsse über einen Menschen, die zu spürbaren Auswirkungen auf das Leben des Einzelnen führen können.

Die Studie

Diese Studie identifiziert die Datenschutzprobleme bei Online-Spielen und zeigt Lösungen auf. Hierzu haben wir aktuelle Spiele für zahlreiche Spieleplattformen auf ihre Datenverarbeitung hin analysiert. Dies betraf die gängigen Konsolen mit den Diensten bzw. Spielsystemen Xbox Live, PlayStation Network und Wii Connect, tragbare (Spiel-)Geräte wie das iPhone, Nintendo DS und PSP, Computerprogramme wie World of Warcraft oder Herr der Ringe Online, Computerspielsysteme wie Valve Steam und auch plattformübergreifende Spiele wie Browsergames und Spiele in Sozialen Netzwerken wie FarmVille.

Besonderes Augenmerk wurde dabei auf die Transparenz der Datenverarbeitung und die Datenschutzerklärungen gelegt. Auch Meinungen und Diskussionen in Fachzeitschriften und

Foren wurden untersucht. Von uns veranstaltete Workshops mit Herstellern und Betreibern von Online-Spielen lieferten weitere Informationen. Besonders wertvoll war eine Umfrage mit mehr als 1.000 Teilnehmern, die wir unter Spielern durchgeführt haben. Insbesondere einige offen gehaltene Fragen, die die Spieler einluden, eigene Gedanken zu dem Thema mitzuteilen, brachten wesentliche Ergebnisse und halfen dabei, Problembereiche zu identifizieren.

Die Ergebnisse wurden auf ihre Relevanz hinsichtlich des geltenden Datenschutzrechts betrachtet. Hierzu haben wir zunächst untersucht, welches (internationale) Recht in welchen Konstellationen zur Anwendung kommt. Im weiteren Verlauf der Studie haben wir dann den Schwerpunkt auf das europäische und das in Deutschland geltende Recht gelegt, das bei den meisten Spielen, die sich an den deutschen Markt richten, anwendbar ist.

Auf Basis dieser Ergebnisse haben wir 27 Einzelfunktionen von Online-Spielen identifiziert, die datenschutzrechtlich relevant sind. Für jede dieser Funktionen haben wir die einschlägigen Datenschutzgesetze identifiziert, deren Regelungsinhalt dargelegt und Hinweise für den praktischen Einsatz gegeben. Daraus entstand ein Datenschutz-Leitfaden für Online-Spiele. Dieser wurde dann mit Herstellern und Betreibern von Online-Spielen in einem Workshop diskutiert, um Rückmeldungen aus der Praxis zu erhalten.

Neben der rechtlichen Einordnung waren für die Studie aber auch die Interessen der Spieler wichtig. Diese wurden frühzeitig eingebunden mittels der o. g. Umfrage, einem Workshop, Vorträgen und Vorlesungen.

Ein eigenes Kapitel der Studie beschäftigt sich mit den sozioökonomischen Aspekten von Datenschutz in Online-Spielen. Abschließend haben wir untersucht, welche Geschäftsmöglichkeiten sich aus dem praktizierten Datenschutz ergeben. Unter der Prämisse, dass Datenschutz in Online-Spielen auch ein Geschäftsmodell sein kann, gehen wir auf mögliche Dienstleistungen und Zertifizierungen ein.

Ergebnisse

a) Rechtsgrundlagen

Betreiber von Online-Spielen im außereuropäischen Ausland müssen sich in der Regel an deutsches Datenschutzrecht halten, wenn sie ihre Angebote direkt (auch) an deutsche Spieler richten. Innerhalb der EU kann im Rahmen des Herkunftslandsprinzip bzw. Territorialprinzip auch nur das Recht des Landes relevant sein, in dem die Daten verarbeitende Stelle (meist der Betreiber der Spiele) ihre Niederlassung hat. Da jedoch das Datenschutzrecht in der EU durch entsprechende Richtlinien in vielen Lebensbereichen vereinheitlicht ist, ergeben sich für die meisten Fälle nur geringe Abweichungen gegenüber dem deutschen Datenschutzrecht.

Bei Online-Spielen handelt es sich um Telemedien, auf die in Deutschland das Telemediengesetz (TMG) Anwendung findet. Dies bezieht sich auf Bestandsdaten und Nutzungsdaten zur Erbringung des Spiels. Darüber hinaus gehende Datenverarbeitung richtet sich in der Regel nach dem Bundesdatenschutzgesetz (BDSG), teilweise auch bei bestimmten Diensten

nach dem Telekommunikationsgesetz (TKG).

Grundsätzlich gilt, dass für die Verarbeitung von personenbezogenen Daten entweder eine Rechtsgrundlage oder die Einwilligung des Spielers vorliegen muss. Ist beides nicht gegeben, so ist die Verarbeitung der Daten rechtswidrig. Typischerweise zulässig ist die Verarbeitung von Informationen für die Vertragsgestaltung oder Abrechnung. Auch die Nutzungsdaten dürfen verwendet werden, um das Spiel zu erbringen oder abzurechnen. Darüber hinausgehende Erhebung und Nutzung von personenbezogenen Daten bedarf jedoch in der Regel der Einwilligung des Spielers. Diese muss informiert und freiwillig erfolgen. Somit ist ein besonderes Augenmerk darauf zu legen, den Spieler über die gewünschte Datenverarbeitung umfassend und verständlich aufzuklären. Dabei ist zu beachten, dass Einwilligungen auch widerrufen werden können.

Betreiber von Online-Spielen müssen ihre Datenverarbeitung auf die erforderlichen Daten beschränken. Grundsätzlich sollten sie sich somit bei jedem erhobenen Datum darüber Gedanken machen, ob dieses für die Diensterbringung wirklich notwendig ist. Hinzu kommt, dass sie für jede Datenerhebung vorab auch einen Zweck festlegen müssen. Eine Abfrage von Daten mit dem Hintergedanken, dass man diese eventuell eines Tages mal für einen unbestimmten Zweck benutzen könnte, ist nicht zulässig. Der Spieler ist bei der Datenerhebung in der Regel über den gewählten Zweck zu informieren. Auch nach der Erhebung bleibt der Spiele-Betreiber in der Pflicht, regelmäßig zu überprüfen, ob inzwischen die Erforderlichkeit für die Speicherung der Daten entfallen ist bzw. der angestrebte Zweck erreicht wurde. In diesem Fall muss er die Daten löschen, sofern kein sonstiges rechtlich geregeltes Aufbewahrungsrecht vorliegt. Eine generelle Pflicht zur Vorratsdatenspeicherung für Daten von Spielern gibt es nicht.

Hinzu kommen Anforderungen, die den Betreiber dazu verpflichten, mittels technisch-organisatorischer Vorkehrungen den unzulässigen Zugriff auf die Daten zu verhindern.

Ausdrücklich im Gesetz (§ 13 Abs. 6 TMG) festgelegt ist, dass die Anbieter auch die anonyme bzw. pseudonyme Nutzung des Spiels ermöglichen müssen. Hierüber müssen sie den Spieler informieren, und es müssen Maßnahmen ergriffen werden, dass Pseudonyme nicht unzulässigerweise aufgedeckt werden.

Die Übermittlung an Dritte bedarf ebenfalls der Einwilligung des Spielers oder einer gesonderten Rechtsgrundlage. Dabei kann kein Konzernprivileg geltend gemacht werden, das größeren Spiele-Betreibern den freien Datenverkehr zwischen Tochterunternehmen und Konzernmutter erlauben würde. Auch dort gelten die allgemeinen Grundsätze des Datenschutzrechts und es bedarf einer gesetzlichen Rechtfertigung bzw. Einwilligung des Betroffenen für die Übermittlung. Innerhalb der EU gibt es jedoch mit dem Instrument der Auftragsdatenverarbeitung eine Möglichkeit, Datenverarbeitungsdienstleistungen auszulagern. Notwendig sind hierfür jedoch insbesondere entsprechend gestaltete Verträge und die sorgfältige Auswahl und Kontrolle des Auftragnehmers durch den Auftraggeber. Sollen darüber hinaus Daten etwa an Werbedienstleister übermittelt werden, ist hierfür die ausdrückliche Einwilligung des Spielers erforderlich.

Zu beachten ist, dass nach deutschem Recht auch die IP-Adresse des Rechners des Spielers ein personenbezogenes Datum ist und damit die Datenschutzgesetze hierauf anwendbar sind. Rechtlichen Problemen kann durch eine umgehende Anonymisierung der IP-Adresse nach Diensterbringung aus dem Weg gegangen werden.

Anonyme Statistiken unterfallen zwar nicht dem Datenschutzrecht. Sobald jedoch Profile unter Pseudonym erstellt werden, muss dem Spieler ein Widerspruchsrecht eingeräumt werden, worüber er aufzuklären ist.

Schließlich müssen die Betreiber von Online-Spielen die Rechte der Spieler auf Auskunft, Berichtigung, Löschung und Sperrung der über sie gespeicherten Daten umsetzen.

Die Kommunikation zwischen den Spielern unterliegt großteils dem Fernmeldegeheimnis und darf nicht überwacht werden. Ausnahmen können sich im Rahmen der Jugendschutzgesetze ergeben, sofern die Spieler über die entsprechenden Einschränkungen informiert wurden.

b) Untersuchung der Spiele

Die Untersuchung einer Auswahl der auf dem Markt befindlichen Spielsysteme und Spiele im Rahmen dieses Vorhabens hat zahlreiche Verstöße gegen die Datenschutzgesetze aufgezeigt. Kaum eine Datenschutzerklärung war so verfasst, dass sie dem Grundsatz der sowohl umfassenden als auch verständlichen Aufklärung entsprach. Einige Betreiber lassen sich dabei weitgehende Rechte an der Verwendung der personenbezogenen Daten einräumen, die nicht im Einklang mit dem Erforderlichkeitsprinzip und Zweckbindungsprinzip stehen. Insbesondere Betreiber außerhalb der EU behandeln die IP-Adresse nicht als besonders schützenswertes Datum. Einwilligungen wurden großteils nur pauschal eingeholt, ohne dass die genauen Auswirkungen für den Spieler immer erkennbar waren. Die Löschung von Daten war teilweise gar nicht oder erst auf wiederholte Nachfrage möglich. Bei der Einbindung in Soziale Netzwerke war nicht immer differenzierbar, welche Daten zu welchem Zweck dem Spiele-Betreiber zur Verfügung gestellt werden.

Einige Spiele übermittelten schon bei der Einrichtung des Spiels Daten an den Betreiber, ohne dass dieses für den Spieler ersichtlich war. Werden im Hintergrund Systeme zur Rechnerüberwachung installiert, so ist oftmals kaum erkennbar, was genau diese Programme überwachen und übermitteln.

Die Verpflichtung zur Einräumung einer pseudonymen bzw. anonymen Bezahlung und Nutzung wird nur von wenigen Betreibern umfassend umgesetzt. Selbst wenn anonyme Bezahlsysteme (Prepaid-Karten) angeboten werden, werden teilweise weitere den Spieler identifizierende Daten erhoben, ohne dass hierfür eine Erforderlichkeit, etwa aus Jugendschutzgründen, erkennbar ist.

Auch Kommunikationsinhalte werden von einigen Betreibern analysiert, teilweise aus Sicherheitsgründen, teilweise zu Werbezwecken.

c) Weitere Ergebnisse

Die Untersuchungen, Gespräche und Umfrage haben gezeigt, dass viele Spieler an dem

Thema Datenschutz interessiert sind. Sie haben das Gefühl, keine wirkliche Kontrolle über ihre Daten ausüben zu können und fühlen sich schlecht informiert. Aber auch die Betreiber sind verunsichert und sind sich teilweise nicht bewusst, welche Datenschutzvorgaben sie einzuhalten haben.

Die datenschutzgerechte Gestaltung von Online-Spielen kann den beteiligten Unternehmen helfen, Vertrauen bei Spielern aufzubauen und diese langfristig an sich zu binden. Audits und Gütesiegel können die Hersteller und Betreiber dabei unterstützen. Wo nicht die technischen und fachlichen Möglichkeiten beim Betreiber für eine datenschutzgerechte Abwicklung des Spielgeschehens gegeben sind, können externe Dienstleister unterstützen.

Ausblick

Während der Erstellung der Studie haben sich zahlreiche neue Entwicklungen auf dem Markt der Online-Spiele ergeben, die neue Datenschutzprobleme mit sich bringen können. So nimmt die Integration von Spielen in Soziale Netzwerke sprunghaft zu. Im Bereich der sog. Casual Games werden auch Gesundheitsdaten wie das eigene Gewicht oder Jogging-Verhalten zu Spieldaten. Bei Online-Spielen auf Mobilgeräten kommen nunmehr auch Standortdaten hinzu, die besonderen rechtlichen Regelungen unterliegen.

Wir stehen in Deutschland immer noch am Anfang der Entwicklung von Online-Spielen zum Massenphänomen. Dies eröffnet aber auch die große Chance, Neuentwicklungen gleich datenschutzgerecht zu gestalten, um so die Fehler, wie bei vielen anderen Online-Dienstleistungen, zu vermeiden.

1 Einleitung

Das Bild des einsamen Videospielers schwindet. Spielen ist heute mehr denn je Kommunikation. Online-Spiele sind ein multimediales Spektakel für die Spieler[1] und bilden mittlerweile eine umsatzstarke Branche innerhalb der Freizeitindustrie. Noch vor Jahren war in Computerspielen die Interaktion nur eingeschränkt möglich. Dagegen verstehen sich die neuen Online-Spiele als virtuelle Welten mit großen Communities. Die Spieler erhalten dabei die Möglichkeit, sich über das Internet zu vernetzen und online miteinander zu spielen. Nicht nur die bekannten Online-Rollenspiele wie World of Warcraft oder Herr der Ringe Online bieten solche Funktionalität, auch die meisten Spiele auf Konsolen, Handhelds und PC ermöglichen inzwischen das Spielen über das Internet. Systemplattformen bzw. Spielsysteme wie Xbox Live[2] oder PlayStation Home[3] unterstützen diesen Community-Gedanken mit umfangreichen Funktionen, die eine vielfältige Vernetzung unter den Spielern ermöglichen. Seit geraumer Zeit finden auch in Sozialen Netzwerken wie Facebook[4] oder StudiVZ[5] Spielsysteme Einzug, die die Kontakte der Spieler innerhalb des Netzwerks in das Spielgeschehen einbeziehen. Diese Entwicklungen bringen eine Vielzahl neuer Spielmöglichkeiten und Geschäftsmodelle mit sich, aber auch vielfältige Herausforderungen. Diese liegen aus Sicht des Datenschutzes darin, dass Hersteller, Publisher und Betreiber von Online-Spielen die datenschutzrechtlichen und datensicherheitstechnischen Anforderungen umsetzen. Gleichzeitig sind die Spieler aufgefordert den Unternehmen kritisch entgegenzutreten.

1.1 Datenschutz in Online-Spielen – „Ich will doch nur spielen“

Online-Spiele sind nicht nur ein Massenprodukt in den Regalen der Händler, sondern haben riesige Fangemeinden. Die Neuerscheinungen der Top-Spiele werden gefeiert wie Musikstars. Online-Spiele gehören zu der heutigen Freizeitindustrie und ziehen Millionen von Spielern in ihren Bann, die ihre Freizeit in einer der Online-Communities verbringen.

Doch sobald Kommunikation stattfindet, weckt diese auch eine Vielzahl von Begehrlichkeiten: Die Spieler hinterlassen in der Online-Welt bei ihren Aktivitäten eine Vielzahl von „verräterischen“ Daten. Diese Daten können zu Spielerprofilen zusammengeführt werden. Die Profile können beispielsweise vermeintlich triviale Informationen wie Spielergebnisse oder

---

1 Unter dem Begriff „Spieler“ verstehen wir sowohl männliche Spieler als auch weibliche Spielerinnen. Auch im Folgenden verwenden wir aus Gründen der einfacheren Lesbarkeit die männliche Sprachform für die Akteure im Zusammenhang mit Online-Spielen, die explizit geschlechtsumfassend zu verstehen ist.

2 Online-Netzwerk der Spielekonsole „Xbox“ vom Hersteller Microsoft.

3 Online-Netzwerk der Spielekonsole „PlayStation“ vom Hersteller Sony.

4 http://www.facebook.de/.

5 http://www.studivz.de/.

Spieldauer enthalten, aber auch weitaus brisantere Informationen, die auf Interessen, Körpergewicht, motorische Schwächen oder Problemlösungsfähigkeiten hindeuten können. Da sich die Spieler bei den meisten Online-Spielen bei der Registrierung identifizieren müssen, sind diese Informationen mit Adressdaten verkettbar[6]. Die Werbewirtschaft hat die neuen Möglichkeiten ebenfalls für sich entdeckt und arbeitet daran, Werbung zielgruppengerecht in die Spiele zu implementieren.

1.2 Datenschutzrecht

Die Erhebung personenbezogener Daten verpflichtet die Daten verarbeitenden Stellen (hier in der Regel die Publisher und Betreiber der Online-Spiele) dazu, die Datenschutzrechte der Betroffenen zu beachten. Dies gilt natürlich auch im Bereich von Online-Spielen. Hier sollen die Datenschutzgesetze die Spieler beispielsweise vor der „Datensammelwut“ der Hersteller oder Betreiber von Online-Spielen schützen.

Die Bestimmung der einschlägigen Rechtsordnung kann bei Online-Spielen aufwendig sein, da eine Vielzahl von unterschiedlichsten Akteuren beteiligt ist. Abhängig vom Sitz eines Herstellers, Publishers oder Betreiber eines Online-Spiels, vom Standort des Servers, auf dem ein Spiel betrieben wird, oder vom gewöhnlichen Aufenthaltsort des Spielers können unterschiedliche nationale oder internationale Rechtsordnungen einschlägig sein. Die Komplexität der Bestimmung und Berücksichtigung der jeweils anzuwendenden Gesetze steigt zumeist mit der Anzahl der beteiligten Staaten. Häufig findet man Situationen vor, bei denen beispielsweise Hersteller des Online-Spiels, Betreiber der Spielserver und die Spieler in unterschiedlichen Ländern ansässig sind.

Abbildung 1: Internationaler Kontext von Online-Spielen

[6] Eine umfassende Darstellung zur Verkettbarkeit von Daten enthält der Report „Verkettung digitaler Identitäten“ des Unabhängigen Landeszentrums für Datenschutz in Zusammenarbeit mit der Technischen Universität Dresden im Auftrag des Bundesministeriums für Bildung und Forschung; 2007. Veröffentlicht unter: https://www.datenschutzzentrum.de/projekte/verkettung/.

Diese Konstellation kommt u. a. dadurch zustande, dass die Online-Spiele für den internationalen Markt konzipiert und entwickelt werden. Die verschiedenen nationalen Versionen weisen zumeist nur geringe Unterschiede auf. Ein Großteil der Anpassung entfällt hierbei auf die Sprache. Für den deutschsprachigen Raum bedeutet dies, dass schlecht übersetzte Datenschutzerklärungen und Defizite in der datenschutzrechtlichen und datensicherheitstechnischen Ausgestaltung von Online-Spielen nicht selten sind.

Das anzuwendende Recht ist nicht nur vom Sitz der Akteure, sondern auch von den Sachzusammenhängen abhängig. Es bietet sich daher an, die Datenschutzanforderungen an Online-Spiele in den folgenden Kapiteln mit dem Blick auf den Zweck der Datenverarbeitung modular zu untersuchen. Die dabei aufgezeigten Lösungen verbinden Datenschutz und Online-Spiele, ohne dass hierbei der Spielspaß oder der Geschäftserfolg auf der Strecke bleiben muss.

In der Studie werden zur Lösung der datenschutzrechtlichen Fragen in Online-Spielen die maßgeblichen Begriffe definiert und erläutert, die vorhandenen Spielsysteme und -arten aufgezeigt mit deren spezifischen Datenschutzfragen die rechtlichen Aspekte hinsichtlich der anwendbaren Rechtsordnungen erörtert.

Sodann werden die datenschutzrechtlichen Grundsätze, die für alle Spiele gelten, aufgeführt und die relevanten Normen für Online-Spiele dargestellt und angewandt.

Im Folgenden ist dann aus den gefundenen Ergebnissen ein Leitfaden entwickelt worden, der die wesentlichen Funktionen von Online-Spielen enthält und eine Darstellung der datenschutzkonformen Anwendung der Funktionen aufführt.

In dem daran anschließenden Kapitel werden Aufbau, Durchführung und Ergebnisse einer Befragung von Spielern zum Thema Datenschutz und Online-Spiele dargestellt. Nach einer sozioökonomischen Betrachtung von Datenschutz und Online-Spielen werden Geschäftsmodelle in diesem Bereich diskutiert.

Die Ausführungen in der Studie beziehen sich primär auf Online-Spiele mit Bezug zum deutschen Rechtssystem. Dies ist erforderlich, da der Rechtsrahmen international nicht ausreichend harmonisiert ist und derartig im Fluss ist, dass eine umfassende Darstellung über die deutschen Grenzen hinaus nicht möglich ist.

2 Grundlagen und Begriffsbestimmung

2.1 Online-Spiele

Als Online-Spiele werden die digitalen Spiele bezeichnet, die alleine oder gemeinsam mit anderen gegen ein oder mehrere Gegner (Mensch oder Maschine) über eine Datennetzverbindung gespielt werden. Als Online-Spiele gelten somit keine Spiele, die zwar Mehrspielerfunktionalität bieten, dafür aber keine Netzverbindung (Internet / LAN) benötigen. Keine Online-Spiele sind beispielweise Spiele an einem Gerät mit mehreren Spielcontrollern[7] oder auch Spiele mit „Hot-Seat-Modus“[8]. Ebenfalls gelten Spiele, die über das Internet heruntergeladen werden, dann im Weiteren aber stationär ohne Netzverbindung gespielt werden, nicht als Online-Spiele im Sinne dieser Studie.[9]

2.2 Hauptakteure bei Online-Spielen

Im Rahmen von Online-Spielen gibt es je nach Spiel und Spielkonzept eine Reihe von beteiligten Akteuren. Bevor die datenschutzrechtlichen Auswirkungen der unterschiedlichen Konstellationen im Rahmen dieser Studie analysiert werden, sollen zum besseren Verständnis die Akteure und ihre Aufgaben kurz beschrieben werden. Akteure sind der Hersteller, der Publisher und der Betreiber des Online-Spiels, weitere Dritte mit zusätzlichen oder unterstützenden Dienstleistungen und der Spieler des Online-Spiels. Dabei können mehrere Akteure in verschiedenen Funktionen auftreten, so dass beispielsweise der Hersteller des Spiels dieses auch verkauft und somit die Aufgaben des Publisher übernimmt.

2.2.1 Hersteller von Online-Spielen

Der Hersteller von Online-Spielen beschäftigt sich hauptsächlich mit der Entwicklung von Online-Spielen. Seine Aufgaben reichen von der Entwicklung der Spielidee bis zur Fertigstellung des auslieferungsreifen Produkts. Dieser Akteur beschäftigt sich also mit den Bereichen Konzeption, Programmierung und Design. Neben dem Begriff Hersteller wird auch das Syn-

---

[7] Controller gehören zum Bereich Hardware und dienen zur Steuerung von Computerspielen. Online-Spiele gehören zur Gruppe der Computerspiele.

[8] Der Hot-Seat-Modus ist ein Spielkonzept, um mit mehreren Personen ein Computerspiel zu spielen, auch wenn nur ein Computer zur Verfügung steht. Dabei werden immer nur die Spieldaten für einen Spieler angezeigt, die anderen Spieler müssen sich in Diskretion üben und wegschauen.

[9] Christoph Kimmert, Computer- und Videospiele, in: Mangold, Roland / Vorderer, Peter / Bente, Gary, Lehrbuch der Medienpsychologie S. 695-716;
Sven Jöckel, Online Spiele – Eine konzeptuelle Abgrenzung verschiedener Spielformen, in: Menschen, Märkte, Medien Management – Berichte aus Forschung und Lehre 02/2007.

onym Entwickler verwendet. In der Regel fallen beim originären Hersteller keine personenbezogenen Daten der Spieler an. Jedoch sollte er schon bei der Entwicklung des Spiels auf eine datenschutzgerechte Gestaltung bedacht sein, um einen rechtskonformen Einsatz zu ermöglichen und zu unterstützen.

2.2.2 Publisher von Online-Spielen

Die Aufgaben des Publishers umfassen hauptsächlich die Vermarktung und den Vertrieb der Online-Spiele. Dabei übergibt der Publisher die Spiele in die klassische Vertriebskette über den Handel oder vertreibt die Spiele direkt an den Endkunden. Die Direktvermarktung findet beispielweise über Online-Portale statt; hier kann der Spieler die Online-Spiele ohne Umwege über den Handel online erwerben und ggf. gleich herunterladen.

2.2.3 Betreiber von Online-Spielen

Die Online-Spiele bieten den Spielern vielfältige Möglichkeiten der Vernetzung mit anderen Spielern. Zumeist wird deshalb eine Online-Plattform bzw. virtuelle Welt als Medium zur Verfügung gestellt, die der Betreiber unterhält. Tätigkeitsfelder des Betreibers sind unter anderem die Bereitstellung von Servern, auf denen die Handlungen der Spieler synchronisiert werden, und der Betrieb von Chats oder Foren, die die Vernetzung der Spieler untereinander fördern. Die Spielserver sind das zentrale Objekt für die Vernetzung der Spieler in virtuellen Welten.

Der Betreiber beim Spielbetrieb ist die Daten verarbeitende Stelle. Im Rahmen des TMG wird er auch als Diensteanbieter bezeichnet (§ 2 Nr. 1 TMG).

Teilweise können auch mehrere Betreiber zur Erbringung eines Online-Spiels auftreten. Dies kann z. B. der Fall sein, wenn durch den Betreiber des eigentlichen Online-Spiels zusätzlich eine Spielplattform bzw. ein Spielsystem genutzt wird, die die Grundfunktionalitäten bzw. die Vermittlung der Spielpartner übernimmt. Dies kann so weit gehend, dass auch die Server und die gesamte Infrastruktur vom Betreiber der Spielplattform bereitgestellt werden, wie es z. B. bei Xbox Live in der Regel der Fall ist (Ausnahmen sind hier die Online-Spiele „Phantasy Star Universe“ und „Final Fantasy XI“, die eigene Server nutzen).

Je nach Konstellation und Auftreten können beide jeweils entsprechend Daten verarbeitende Stelle sein. Wird ein Betreiber durch den anderen beauftragt, so kann eine Auftragsdatenverarbeitung vorliegen, bei der nur der Auftraggeber verantwortliche Stelle ist.

2.2.4 Spieler von Online-Spielen

Der Spieler ist der Endkunde im Bereich Online-Spiele und verbringt mehr oder weniger Zeit mit dem Spielen von Online-Spielen. Dabei steht er ggf. in vertraglichen Beziehungen mit dem Publisher beim Kauf des Spiels und mit dem Betreiber beim eigentlichen Spielbetrieb. Neben dem Begriff Spieler wird auch das Synonym User, Nutzer (vgl. § 2 Nr. 3 TMG) oder

Betroffener (vgl. § 1 Abs. 1 BDSG) verwendet.

2.2.5 Dritte

Auf der Seite der Unternehmen gibt es neben den klassischen Hauptakteuren noch weitere beteiligte Dritte, die unterschiedliche Dienstleistungen zur Verfügung stellen. Hierzu gehören beispielsweise Unternehmen der Werbewirtschaft, die sich mit der Vermarktung und technischen Realisierung des In-Game-Advertisings, oder Payment-Organisationen, die sich mit der Abwicklung des Zahlungsverkehrs in Online-Spielen befassen. Letztere ermöglichen es, die Abo-Gebühren für ein Online-Spiel per Kreditkarte oder anonymem Prepaid-Karten-System einzuziehen.

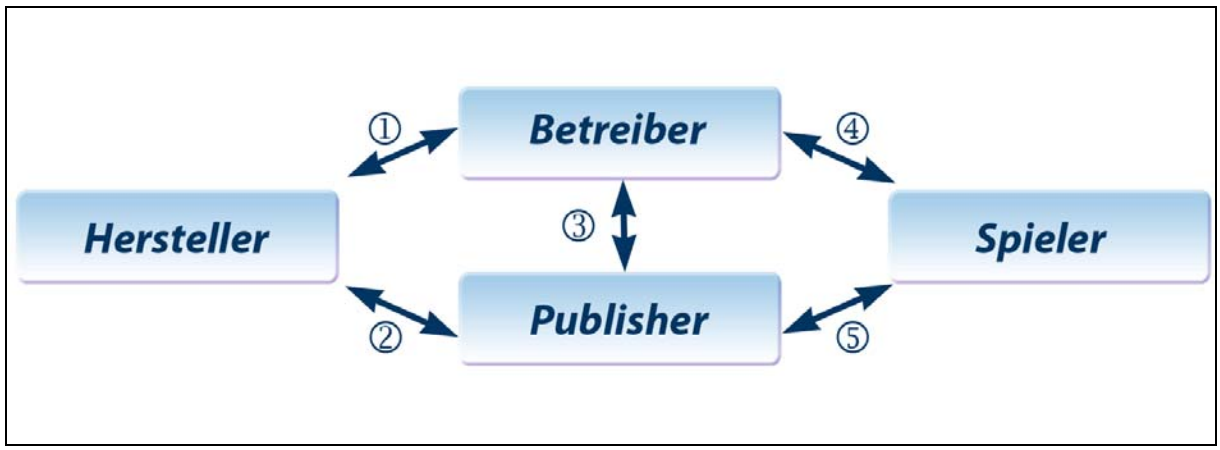
Dritte können auch weitere Nutzer des Spiels oder auch sonstige Personen oder Organisationen sein, die Einsicht in z. B. Spielerprofile nehmen könnten.

2.2.6 Klassische Verknüpfung der Hauptakteure

Im Bereich der Online-Spiele ergeben sich somit die folgenden klassischen Verknüpfungen zwischen den Akteuren, die in Abb. 2 veranschaulicht werden. Dabei können die Aufgaben mehrerer Akteure von einer Organisation wahrgenommen werden. Es handelt sich im Folgenden um eine typische Konstellation.

Der Hersteller entwickelt das Online-Spiel und überlässt dieses dem Publisher zur Vermarktung. Der Betreiber sorgt für den reibungslosen Betrieb des Online-Spiels. Der Spieler erwirbt das Spiel direkt beim Publisher oder im Handel[10]. Beim eigentlichen Spielen verbindet sich der Spieler dann mit den Servern des Betreibers.

Abbildung 2: Typische Beziehungen zwischen den Akteuren



[10] In der nachfolgenden Grafik wird die Direktvermarktung des Publishers an den Kunden beispielsweise über ein Online-Portal dargestellt, der Vertriebsweg über den Handel wird nicht betrachtet.

Die typischen Beziehungen zwischen den Akteuren lassen sich wie folgt beschreiben:

1: Der Hersteller stellt (ggf. gegen Bezahlung) dem Betreiber die Serverkomponente des Spiels zur Verfügung.

2: Der Hersteller stellt dem Publisher (ggf. gegen Bezahlung) die Enduser-Version des Spiels zum Weitervertrieb zur Verfügung.

3: Der Publisher integriert ggf. das Spiel in das Spielsystem des Betreibers (ggf. gegen Bezahlung). Der Betreiber meldet u. a. Informationen über die Anzahl der Spieler an den Publisher zurück.

4: Der Spieler meldet sich beim Betreiber zum Spielen an und verbindet sich zum Spielen mit dessen Servern (ggf. gegen Bezahlung).

5: Der Publisher stellt dem Spieler die Clientversion des Spiels zur Verfügung (ggf. gegen Bezahlung).

2.3 Grundlagen Datenschutzrecht

2.3.1 Personenbezogene Daten

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Dazu gehören neben dem Namen und dem Geburtstag unter anderem auch Angaben zur Anschrift, zum Beruf und zu privaten Aktivitäten[11]. Ob ein Datum personenbezogen ist oder nicht, hängt in erster Linie davon ab, ob dieses Datum Aussagen zu bestimmten oder bestimmbaren Personen zulässt. Insoweit können auch Bild- und Tonaufnahmen personenbezogene Daten darstellen. Für Online-Spiele von Bedeutung sind daneben auch Daten zum Nutzungs- und Spielverhalten und IP-Adressen, die der Computer automatisch zum Verbinden mit dem Internet generiert.

2.3.2 Automatisierte Verarbeitung

Gemäß § 1 Abs. 2 Nr. 3 BDSG findet das BDSG Anwendung, wenn die personenbezogenen Daten durch nicht-öffentliche Stellen, vorliegend die Publisher und Betreiber von Online-Spielen, personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen erheben, verarbeiten oder nutzen.

Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG).

Verarbeiten ist nach § 3 Abs. 4 BDSG das Speichern, Verändern, Übermitteln, Sperren und

[11] Tinnefeld / Ehmann / Gerling, Einführung in das Datenschutzrecht, 4. Auflage 2005, S. 279.

Löschen personenbezogener Daten. Dabei ist Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung auszuschließen. Und Löschen ist das Unkenntlich machen gespeicherter personenbezogener Daten.

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (§ 3 Abs. 5 BDSG).

Durch das Anmelden bzw. Einloggen, das Speichern der (Nutzungs-) Daten der (fiktiven) Spielercharaktere und das gegebenenfalls erforderliche Abrechnen der Online-Spielzeiten erfolgt bei Online-Spielen eine entsprechende Datenerhebung, -verarbeitung und -nutzung.

2.3.3 Verantwortliche Stelle

Verantwortliche Stelle gemäß § 3 Abs. 7 BDSG ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Da das nationale Recht richtlinienkonform auszulegen ist, ist für eine weitere Präzisierung Art. 2 Abs.1 lit. d) der EG-Datenschutzrichtlinie[12] heranzuziehen; danach ist nur verantwortlich, wer Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung hat.

2.3.4 Nutzer / Betroffener

Der Nutzer ist jede natürliche Person, die Online-Spiele und die technischen Voraussetzungen nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen (vgl. § 2 Nr. 3 TMG). Da die personenbezogenen Daten des Nutzers erhoben, verarbeitet und genutzt werden, ist der Nutzer auch Betroffener im Sinne des § 3 Abs. 1 BDSG. In dieser Studie ist dies zumeist der Spieler von Online-Spielen.

2.3.5 Diensteanbieter

Der Diensteanbieter ist jede natürliche oder juristische Person, die eigene oder fremde Online-Spiele (Telemedien) zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (vgl.

[12] Richtlinie 95/46/EG Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABL. EG Nr. L 281 vom 23.11.1995, S. 31-50.

§ 2 Nr. 1 TMG). In dieser Studie handelt es sich bei dem Diensteanbieter zumeist um den Betreiber von Online-Spielen.

Ein Access-Provider ist ebenfalls Diensteanbieter, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt (§ 3 Nr. 6 Telekommunikationsgesetz (TKG)).

2.3.6 Server

Server sind technische Einrichtungen oder Systeme, die Datenverarbeitung ermöglichen und auch als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (vgl. § 3 Nr. 23 TKG). Server dienen dem Angebot von Telekommunikationsdiensten und Telemediendiensten.

2.4 Grundlagen im Bereich Online-Spiele

2.4.1 Hardware

Die verschiedenen Online-Spiele (Software) werden für verschiedene Plattformen (Hardware) entwickelt oder angeboten. Einige Spiele werden für verschiedene Plattformen entwickelt, andere Spiele werden dagegen exklusiv nur für eine Plattform angeboten. Die Plattformen lassen sich dabei in die folgenden Kategorien einteilen:

Tabelle 1: Plattformen (Hardware) für Online-Spiele (Auswahl)

Plattform	Beispiele	Kurzform
Klassischer Computer	PC (Windows, Linux etc.) oder Apple Macintosh	
Stationäre Spielkonsole	Gamecube (Hersteller: Nintendo)	
	PlayStation 1, 2 und 3 (Hersteller: Sony)	PS 1, PS 2, PS 3
	Wii (Hersteller: Nintendo)	
	Xbox und Xbox 360 (Hersteller: Microsoft)	
Mobile Spielkonsole	Nintendo DS (Hersteller: Nintendo)	NDS
	PlayStation Portable Go (Hersteller: Sony)	PSP Go
	PlayStation Portable (Hersteller: Sony)	PSP
Handheld	Handy (z. B. Apple iPhone, Nokia) oder PDA / iPad	

Zusätzlich werden Online-Spiele für Browser angeboten, die auf vielen der o. g. Plattformen genutzt werden können und systemunabhängig sind.

2.4.2 Online-Netzwerke

Die Marktführer im Bereich der Spielkonsolen bieten für ihre Konsolen eigene Online-Netzwerke an, die eine Vielzahl von Online-Funktionalitäten für die Spielkonsolen bereitstellen. Diese Netzwerke dienen zumeist dazu die Spieler untereinander in einer Online-Community zu vernetzen und weitere Produkte für die Spielkonsole zu vermarkten. Diese Netzwerke werden im Folgenden den Spielkonsolen zugeordnet:

Tabelle 2: Online-Netzwerke von Spielkonsolen (Auswahl)

Online-Netzwerk	**Spielkonsole**
Xbox Live (Microsoft)	Xbox Xbox 360
PlayStation-Network (PSN) (Sony) PlayStation Home (Sony) (Erweiterung des PSN um eine virtuelle Welt)	PlayStation 3 PlayStation Portable PlayStation Portable Go PlayStation 3
WiiConnect24 (Nintendo)	Wii

2.4.3 Avatar und virtuelle Welt

Der Avatar ist die Spielfigur des Online-Spielers. Je nach Online-Spiel und der dahinterstehenden Funktionalität gestaltet der Spieler im Spiel diesen Avatar als seinen virtuellen Spiel-Charakter.

In einigen Online-Spielen steht als Spielfeld eine simulierte Umgebung, die meist an der realen Welt angelehnt ist. (virtuelle Welt) zur Verfügung. Insbesondere in einem Massively Multiplayer Online Role-Playing Game (MMORPG) (Massen-Mehrspieler-Online-Rollenspiel) ist die virtuelle Welt ein entscheidender Spielbestandteil. Die virtuelle Welt ist ein virtuelles Abbild einer Gesellschaftsstruktur, in der sich die Avatare als Bewohner aufhalten und Aufgaben erfüllen.

2.5 Arten von Online-Spielen

In der Wissenschaft gibt es derzeit keine einheitliche, fachübergreifende und sich durchsetzende Klassifizierung von Online-Spielen. Es zeigt sich, dass die verschiedenen Forschungsrichtungen die bestehenden Klassifizierungen anpassen oder neue Klassifizierungsschemata für ihr Fachgebiet entwickeln.

2.5.1 Allgemeiner Ansatz der Klassifizierung

Eine einfache Klassifizierung für Computerspiele nutzt die Unterhaltungssoftware Selbstkontrolle (USK). Die USK ist in Deutschland die verantwortliche Stelle für die Überprüfung von an Datenträger gebundenen Computerspielen mit entsprechender Altersfreigabe, § 14 Jugendschutzgesetz (JuSchG). Die USK teilt Computerspiele in die folgenden Genres von Spielen ein:

Tabelle 3: Klassifizierung von Computerspielen

Spielgenre[13]	**Beschreibung**[14]
Action-Adventure	Lösen von abenteuerorientierten Rätseln mit geschicklichkeitsfordernden Spielelementen
Klassisches Adventure	Lösen von abenteuerorientierten Rätseln durch Logik ohne Zeitdruck
Arcade	Einfaches Spielkonzept mit Fokus auf Geschick und Reaktionsfähigkeit
Denkspiel	Geschicklichkeitsspiele mit Forderung der Kombinationsgabe
Genremix	Kombination von verschiedenen Genres
Gesellschaftsspiel	Computerspiel, basierend auf bekannten klassischen Spielvorlagen
Jump 'n Run	Spielkonzept basiert auf Schnelligkeit und Geschicklichkeit in verschiedenen Spielwelten
Kinder-/Kreativ	Einfache bunte Aufgaben fordern und trainieren Fähigkeiten
Management	Simulation von Wirtschaftsabläufen
Rollenspiel	Der Spielcharakter erfüllt Aufgaben in virtuellen Fantasiewelten
Shooter	Das Spielkonzept basiert auf dem Eliminieren von gegnerischen Spielfiguren
Simulation	Nachvollziehen von lebensechten komplexen Zusammenhängen
Sportspiel	Realitätsnahes Nachspielen von echten Sportarten
Strategie	Planerisches Spielgeschehen mit gezieltem Einsatz der unterschiedlichen Ressourcen

Diese Klassifizierung von Spielen ist für die Betrachtung des Datenschutzes und der Datensicherheit bei Online-Spielen kein geeigneter Ansatzpunkt. Sie orientiert sich am Spielerlebnis für den Spieler und dessen Herausforderung während des Spielvorgangs und ist losgelöst von der Online-Nutzung und Fragen des Datenschutzes.

[13] Spielgenres wurden entnommen von der Internetpräsenz der USK; http://www.usk.de/.

[14] Beschreibung der Spielgenres in Anlehnung an die Beschreibung auf der Internetpräsenz der USK; http://www.usk.de/.

2.5.2 Klassifizierung von Online-Spielen nach dem Umfang der Datenerhebung

Ein aus Sicht des Datenschutzes zweckmäßigerer Ansatz ist die Klassifizierung der Online-Spiele nach dem Spielsystem in Bezug auf den daraus resultierenden Umfang der Datenerhebung. Es haben sich hierbei drei Kategorien von Spielsystemen herausgebildet. Bei diesen Spielsystemen werden jeweils in unterschiedlicher Form und in unterschiedlichem Umfang personenbezogene Daten erhoben.

Die Spielarten lassen sich wie folgt kurz systematisieren:

Private Netze

Die privaten Netze zeichnen sich dadurch aus, dass die Vernetzung einzig zwischen den Nutzern aufgebaut wird, ohne dass eine außenstehende dritte Person in den Betrieb involviert ist. Die Daten bleiben damit im persönlichen Umfeld, so dass schon von daher die Anwendung der Datenschutzgesetze ausscheidet (vgl. § 1 Abs. 2 Nr. 3 BDSG). Solche Netze haben aus Datenschutzsicht den Vorteil, dass keine bzw. nur sehr wenige personenbezogene Daten erhoben werden und keine Dritten, auch keine (kommerziellen) Betreiber, involviert sind, die ein wirtschaftliches Interesse an einer Verwertung von personenbezogenen Daten haben.

Geschlossene Systeme

Bei geschlossenen Spielsystemen, die von einem Betreiber unterhalten werden wie beispielsweise Xbox Live von Microsoft oder PlayStation-Network von Sony fallen in der Regel zahlreiche Daten über die Person des Spielers, sein Spielverhalten, seine Kommunikation und Kontakte an. Für zusätzliche Leistungen können weitere Betreiber variabel an das zentral verwaltete System angebunden werden. Dies geschieht beispielweise wenn für Online-Spiele separate Spielserver zur Verfügung stehen. Bei geschlossenen Systemen fallen personenbezogene Daten an, an denen die Betreiber ein wirtschaftliches Interesse haben. Es ist darauf zu achten, dass die Verarbeitung der personenbezogenen Daten transparent und rechtlich einwandfrei erfolgt.

Offene Systeme

Die Systemarchitektur bei offenen Systemen lässt eine beliebige Anzahl von Betreibern zu. Wie bei den geschlossenen Systemen fallen in der Regel eine Vielzahl von personenbezogenen Daten an. Als Beispiel lassen sich hier Peer-to-Peer Netze[15] anführen. Aus Datenschutzsicht besonders problematisch ist die geringe Transparenz solcher Systeme. Dem Nutzer bleibt verborgen, mit wie vielen Betreibern er in Verbindung steht und welcher Betreiber welche Daten erhebt.

Im Folgenden werden die drei kurz vorgestellten Spielsysteme ausführlicher dargestellt und einzelne Datenschutzproblematiken beispielhaft thematisiert.

[15] In einem Peer-to-Peer Netz nehmen die Clients sowohl Dienste in Anspruch und bieten gleichzeitig Dienste an. Im Gegensatz zu einem Client-Server-Netz, wo der Server Dienste anbietet und der Client dieses Dienste in Anspruch nimmt.

2.5.2.1 Private Netze

Bei privaten Netzen wird die Verbindung zum Spielen zwischen den Spielern selbst etabliert. Wurden früher hierzu eigene Netze aufgebaut, wird heute in der Regel für die Verbindung der Rechner das Internet verwendet. Da sich der Aufbau und der Datenaustausch in solchen Netzen im persönlichen Umfeld abspielen, finden die Datenschutzgesetze keine Anwendung (vgl. § 1 Abs. 2 Nr. 3 BDSG). Der Nutzer sollte auch im persönlichen Umfeld darauf achten, welche Daten er für sein privates Umfeld zugänglich macht.

2.5.2.2 Geschlossene Systeme

In geschlossenen Online-Spielsystemen können durch den Betreiber zahlreiche Daten über das Spielverhalten der Nutzer gesammelt werden. Der Nutzer kann diese zumindest teilweise selbst einsehen, aber auch, vergleichbar zu Sozialen Netzwerken, anderen zur Einsicht freischalten, sofern diese Daten nicht schon standardmäßig freigegeben sind. Damit haben dann ggf. zahlreiche Spieler Einblick in personenbezogene Daten. Dies kann etwa die zuletzt gespielten Spiele, die erreichten Spielziele oder besondere Leistungen im Spiel betreffen.

Es kann für bestimmte Unternehmen oder Personen von Bedeutung sein, welche Spiele gespielt wurden, nicht nur für die eventuell zielgruppenorientierte Werbung, sondern auch für potentielle Arbeit- oder Auftraggeber. Von besonderer Bedeutung ist das jeweilige aufgezeichnete Spielverhalten eines Spielers. Das Spielverhalten selbst kann Rückschlüsse auf den Spieler zulassen. Informationen, die virtuelle Identitäten betreffen, könnten mit Daten aus dem realen Leben eines Spielers kombiniert werden und so zu Aussagen über die reale, hinter der virtuellen Identität stehende, natürliche Person treffen. Dies könnte die Art und Weise an das Herangehen und Lösen von Aufgaben, Interessen, das Reaktionsvermögen, die Mentalität, das Fahrverhalten, das Kaufverhalten, die Zahlungswilligkeit, den bevorzugten Aufenthaltsort und weitere im realen Leben auftretende alltägliche Fragen betreffen.

In geschlossenen Systemen kann ggf. zwischen den Spielern kommuniziert werden. Hierbei können Textbotschaften, Audionachrichten, Bilder und Videos untereinander ausgetauscht werden.

Viele Spielkonsolen lassen sich zusätzlich mit Videokameras ergänzen, einige Modelle werden bereits standardmäßig mit Kameras ausgeliefert (z. B. Nintendo DSi, iPhone). In diesen Fällen ist eine Beobachtung zwischen den Spielern möglich. Da es in derartigen Situationen auch zu Belästigungen kommen kann, ist eine Verpflichtung zur Überwachung der Spiele oder einer Rückverfolgung der Spieler grundsätzlich gerade bei Spielen, die sich an Kinder und Jugendliche richten, denkbar und muss ggf. mit dem Fernmeldegeheimnis abgewogen werden. Die Überwachung würde zu weiteren Datenerhebungen führen und einen erneuten Datenfluss über den Spielzweck hinaus ermöglichen. Außerdem muss die Aktivierung der Kamera für den Spieler transparent sein.

Neben der Kommunikation zwischen den Spielern ist bei einigen Betreibern eine Bewertung der einzelnen Spieler auf den Spielplattformen möglich. Auch hier sind datenschutzkonforme Lösungen erforderlich. Mitspieler dürfen bei negativen Bewertungen nicht befürchten müs-

sen, nur deshalb selbst derartige Bewertungen zu erhalten. Andererseits sind Verfahren zu etablieren, mit denen unberechtigte Bewertung (z. B. bei Schmähkritik) unverzüglich wieder entfernt werden können.

2.5.2.3 Offene Systeme

Bei offenen Systemen können neben (kommerziellen) Betreibern auch Dritte Spieleserver in die Spieleinfrastruktur einbinden. Dies erfolgt im Rahmen des eingesetzten Kommunikationsprotokolls. Zentrale Verwaltungsserver können die vorhandenen Server managen und die Verteilung auf die Spieler regeln.

Im Gegensatz zu den geschlossenen Systemen ist für den Spieler nicht immer ersichtlich, wer gerade Daten verarbeitende Stelle ist. Insbesondere bei Systemen, die auf dem Prinzip von Peer-to-Peer Netzwerken beruhen, werden die eingesetzten Server dynamisch zugewiesen. Hinzu kommt, dass Daten zwischen den Server ausgetauscht werden können, um z. B. eine einheitliche Spielewelt zu generieren. Die Betreiber von Verwaltungsservern können Daten verarbeitende Stelle hinsichtlich der Anmeldedaten des Spielers sein. Läuft das Spiel selber dann auf den Servern der anderen Betreiber, so sind diese diesbezüglich Daten verarbeitende Stellen. Jeder Betreiber eines Rechners in einem offenen System muss die entsprechend geltenden Datenschutzgesetze beachten. Das System muss so gestaltet sein, dass der Fluss von personenbezogenen Daten für den Spieler nachvollziehbar bzw. transparent ist.

2.5.2.4 Massively Multiplayer Online Games (MMOGs)

Bei den MMOGs handelt es sich um eine besonders populäre Form der Online-Spiele, diese werden sowohl in geschlossenen als auch offenen Systemen angeboten. Aufgrund der Verbreitung von MMOGs wird ihnen hier außerhalb der Einteilung in geschlossene und offene Systeme ein Kapitel gewidmet.

MMOGs stellen den Spielern virtuelle Welten zur Verfügung. Im Rahmen dieser Konstellationen treten umfangreiche datenschutzrelevante Übermittlungen und Erhebungen von Daten auf. Einerseits erhebt der Betreiber der Online-Spiele Daten bei dem Spieler, andererseits werden den Spielern Daten anderer Spieler zur Verfügung gestellt. Dabei kann es sich um reale Daten der Spieler handeln, aber auch um Daten aus der virtuellen Welt, die Rückschlüsse auf die hinter der Spielfigur stehenden Personen zulassen. Die erfassten Daten können es zulassen, umfangreiche Interessenprofile der Spieler aus der Kombination der realen Daten und der Daten der virtuellen Figur zu erstellen. Diese Spiele bieten auch die Möglichkeit, in der virtuellen Welt Werbung für Produkte der realen Welt zu schalten (In-Game-Advertising) und so die Welten zu verbinden und zielgruppenorientierte, auf Profile abgestimmte, Werbung zu betreiben. Die erhobenen Daten könnten somit für Marketingzwecke genutzt werden. In diesem Zusammenhang ist die Nutzung von Avataren von elementarer Bedeutung. Diese sind ggf. in der Lage, Informationen von Nutzern zu protokollieren, deren Avatare sich in ihrer Umgebung in der virtuellen Welt befinden. Dies betrifft dann nicht

nur Verhaltensmuster und Interessen, sondern auch Gesprächs- und Videoaufzeichnungen. Im Einzelfall kann es bei längerfristiger Beobachtung möglich werden, die Identität eines hinter einer Spielfigur stehenden Spielers aufzudecken, wenn genügend Daten für ein Gesamtbild gesammelt und miteinander verbunden werden konnten.

2.5.3 Klassifizierung von Online-Spielen nach datenschutzrelevanten Funktionen

Die Klassifizierung von Online-Spielen nach dem Umfang der Datenerhebung kann aufgrund der groben Untergliederung in drei Kategorien nur ein erster Ansatz sein. Für eine weitergehende Bearbeitung der Datenschutzthematik in Online-Spielen bedarf es einer feiner graduierten Unterteilung, anhand derer die Datenschutzanforderungen an Online-Spiele modular behandelt werden können.

Es ergeben sich nach eingehender Analyse der am Markt aktuell angebotenen Online-Spiele, der sich abzeichnenden Trends auf dem Spielemarkt und den Erfahrungen der aufsichtsbehördlichen Tätigkeit die im Folgenden vorgestellten Module. Hierbei handelt es sich um Funktionen, die ein Online-Spiel aufweisen kann und die besondere datenschutzrechtliche Relevanz haben. Einige davon sind für alle Online-Spiele relevant (z. B. die generellen Vorkehrungen und technisch-organisatorischen Maßnahmen). Andere beziehen sich speziell auf bestimmte Funktionalität (z. B. Ligamodus) und besondere technische Ausstattungen (z. B. Webcams). Die identifizierten datenschutzrechtlichen Funktionen wurden dabei als Module konzipiert. Der Vorteil der Modulbildung ist darin zu sehen, dass die Module separat behandelt werden können und die Beteiligten (Hersteller, Publisher, Betreiber und Dritte) nur die für ihr Produkt oder Leistungsangebot maßgeblichen Module näher betrachten müssen. Der Betreiber etwa, der kein In-Game-Advertising anbietet, kann dieses Modul vernachlässigen. Es kommt durch den modularen Aufbau aber dazu, dass sich einzelne Funktionen bzw. Module teilweise überschneiden.

In Online-Spiele lassen sich folgende datenschutzrelevante Module identifizieren:

Generelle Vorkehrungen

Die generellen Maßnahmen umfassen insbesondere technisch-organisatorische Maßnahmen, die im Umfeld der Erhebung, Verarbeitung und Nutzung personenbezogener Daten notwendig sind, um die datenschutzgerechte und sichere Erhebung, Verarbeitung und Nutzung dieser Daten zu erreichen.[16]

Vertrieb

Beim Vertrieb des Online-Spiels werden Daten der Käufer verarbeitet. Insbesondere beim Online-Vertrieb fallen neben den klassischen Adressdaten weitere auf dem Internetvertrieb basierende Daten (IP-Adressen, E-Mail-Adresse, PC-Ausstattung etc.) an.

[16] Ernestus, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 9, Rn. 20.

Installation und Registrierung

Im Rahmen der Installation und Registrierung werden von dem Spieler Daten direkt und indirekt erhoben. Die direkte Datenerhebung erfolgt beispielweise über eine Abfrage über Formularfelder. Im Gegensatz dazu werden die Daten bei einer indirekten Erhebung nicht unmittelbar beim Spieler abgefragt, sondern beispielsweise über einen Scan des Spielerrechners (Hardwareausstattung, Seriennummern von Komponenten, installierte Software) Daten gesammelt sowie IP-Adressen und Cookie-Inhalte erfasst.

Betrieb und Überprüfung

Während des Online-Spielens werden Daten vom Spiel zum Betreiber übersendet, u. a. um Spielaktionen auszutauschen, den ordnungsgemäßen Betrieb des Online-Spiels zu überprüfen und etwaige (technische) Manipulationen auszuschließen bzw. aufzudecken.

Bezahlsystem

Im Rahmen von Online-Spielen sind Bezahlsysteme etabliert, die den Bezahlvorgang beispielsweise für regelmäßige Gebühren oder punktuell für einzelne zusätzliche Funktionalität (wie z. B. „Item Shopping“) abwickeln. Die Zahlvorgänge können sowohl personalisiert (z. B. Kontoabbuchung, Kreditkartenzahlung) oder anonym/pseudonym (z. B. Prepaid-Karten) erfolgen.

Kündigung / Spielbeendigung

Dieser Punkt umfasst den Umgang mit den Spielerdaten nach einer Kündigung oder der Löschung eines Accounts.

Spieler-zu-Spieler-Erkennbarkeit

In Online-Spielen ist vielfach die Möglichkeit implementiert, innerhalb des Spiels nach anderen Spielern zu suchen und diese im Spiel wiederzuerkennen. Die Spieler können dabei vergleichbar mit anderen Sozialen Netzwerken Profile hinterlegt haben.

Reputationssystem / Beschwerdemanagement

Reputationssysteme in Online-Spielen bieten die Möglichkeit, Mitspieler beispielweise in Hinblick auf Spielverhalten, Fairness oder Einhaltung der Spielregeln zu bewerten. Ein solches Bewertungssystem soll den zumeist unter Pseudonym auftretenden Spielern die Gelegenheit geben, soziale Kontrolle untereinander auszuüben.

Highscoreliste

Highscorelisten dienen der Präsentation von Spielergebnissen. Einblick in diese Listen haben die Spieler, darüber hinausgehend oftmals auch die gesamte Öffentlichkeit.

Ligamodus

Eine besondere Art der Präsentation von Spielergebnissen ist der Ligamodus. Er zeichnet sich dadurch aus, dass über mehrere Spiele oder Partien Punkte gesammelt werden, aus denen ein Ranking erstellt wird. In der Regel setzen sich die Partien aus Spielen zwischen Teilnehmern der entsprechenden Liga zusammen.

Eigenpräsentation des Spielers

Die Leistungspräsentation in Online-Spielen umfasst die Möglichkeit für einen Spieler, seine Spielhistorie und Spielleistungen den anderen Spielern oder der Öffentlichkeit zu präsentieren.

Upload

Spiele können die Funktion anbieten, dass der Spieler eigene Inhalte in das Spielsystem einfügt bzw. hochlädt, sei es zur Beeinflussung der eigenen Spielerfahrung oder um sie Mitspielern zur Verfügung zu stellen. Dies können Fotos, Grafiken, Musikstücke oder sogar zu eigene Level- und Spieldesigns sein.

Chat

Die Chat-Funktion umfasst alle Arten der elektronischen Kommunikation (Text-, Audio- und Videonachrichten) in Echtzeit.

Nachrichtenaustausch

Die Funktion des Nachrichtenaustausches umfasst alle Arten der elektronischen Kommunikation (Text-, Audio- und Videonachrichten), die nicht in Echtzeit, d.h. zeitverzögert bzw. zum späteren Abruf, stattfindet.

Datenschutzkonfiguration

Die Datenschutzkonfiguration ermöglicht es den Spielern, die Verarbeitung ihrer Daten durch den Betreiber und Dritte selbst einzustellen. Dies betrifft z. B. die Speicherfristen, die Weitergabe von Daten an Dritte und die Abrufbarkeit von Daten durch Jedermann etwa über das Internet.

Datenschutzerklärung

Verarbeiten Online-Spiele personenbezogene Daten, so ist der Spieler u. a. über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten zu informieren. Diese Informationen werden in der Datenschutzerklärung zusammengefasst.

Weiterleitung von Daten an Dritte

Dieser Punkt behandelt die Weitergabe von Daten an Dritte und deren weitere Verarbeitung. Beispielhaft hierfür sind die externe Rechnungsstellung, Inkassoverfahren und (personalisierte) Werbung.

In-Game-Advertising

In-Game-Advertising beschäftigt sich mit der statischen oder dynamischen Einbindung von Werbung in Computerspielen. Je nach Vermarktungskonzept sind neben dem Spiele-Hersteller oder -Betreiber weitere Unternehmen eingebunden.

Altersverifikation und Jugendschutz

Zum Schutz vor jugendgefährdenden Inhalten hat der Betreiber von Online-Spielen geeignete Maßnahmen zu ergreifen, um Jugendlichen den Zugang zu solchen Online-Spielen zu

verwehren. Aus diesem Grund werden altersverifizierende Daten vom Spieler abgefragt.

Suchtprävention

Als Maßnahme zur Suchtprävention kann gefährdeten Personen (ggf. auf eigenen Wunsch) der Zugang zu bestimmten Online-Spielen verwehrt werden. Hierzu kann Bedarf daran bestehen, etwa Sperrlisten einzurichten.

(In-Game-)Shopping

In Online-Spielen kann dem Spieler die Möglichkeit gegeben werden, virtuelle oder reale Produkte zu erwerben.

In-Game-Verhaltensanalyse

Die Betreiber können ein Interesse daran haben, das Spielerverhalten zu analysieren, um das Spiel zu optimieren, Werbung bedarfsgerecht zu platzieren oder den Erfolg eines Spiels oder bestimmter Spielteile zu ermitteln (Statistik). Im Gegensatz zu dem Modul „Betrieb und Überprüfung“ geht es hierbei nicht um Funktionalitäten, die das selbst Online-Spiel ermöglichen, sondern um Datenverarbeitung zum Zwecke der späteren Anpassung des Spiels an die Ergebnisse der Analyse.

Webcam / Videoaufzeichnung

Einige Online-Spiel-Konzepte sehen die Einbindung von Webcams vor, um eine Kommunikation unter den Spielern zu ermöglichen oder Foto- oder Videosequenzen in das Spiel zu integrieren.

Always-Online-Funktionalität

Einige Spielkonsolen sind ständig mit dem Internet oder einem Online-Portal verbunden, auch wenn sich die Spielkonsole etwa im Standby-Modus befindet. Hiermit kann eine Überwachung der privaten Lebensgewohnheiten eines Spielers verbunden sein.

Mobile-Gaming

Portable Spielkonsolen und Handys ermöglichen das Spielen an fast jedem Ort. Es werden in der Regel Mobilfunknetze oder WLAN-Netze für das Online-Spielen verwendet. Hierbei kann u. a. der Aufenthaltsort des Spielers als weiteres Datum erhoben und verarbeitet werden.

Spielen über Internet

Viele Online-Spiele nutzen für den Datenaustausch mit dem Spielserver oder mit Mitspielern das Internet. Hierbei fällt zumeist eine Reihe von Daten des Spielers und seines Rechners, wie die IP-Adresse, an.

Einbindung in Soziale Netzwerke

Einige Online-Spiele sind Bestandteile von Sozialen Netzwerken. Dabei greifen die Spiele auf die Struktur der Sozialen Netzwerke und ggf. auf die Kontaktdaten von Nutzern in den Sozialen Netzwerken zu.

Bei der Bestimmung der Module wurde darauf geachtet, dass sie die typischen Datenschutzproblematiken bei Online-Spielen widerspiegeln. Die Datenschutzaspekte der einzelnen Module werden im Rahmen des Leitfadens (siehe Kapitel 9) detailliert erörtert. Die Module können sich in Einzelfällen dabei inhaltlich überschneiden.

3 Online-Spiele – ein Überblick aus Datenschutzsicht

3.1 Einleitung

Wer in die Welt der Online-Spiele einsteigen will, muss sich im Vorwege für die Hardware entscheiden, auf der er das Spiel spielen möchte. Dafür steht neben dem klassischen PC oder Notebook eine Reihe von Spielkonsolen und mobilen Geräten wie Handys zur Verfügung. Die Entscheidung für ein System hat unter Umständen schon erste Auswirkungen auf die Datenschutzkomponenten der später erworbenen Online-Spiele, da je nach Hardware unterschiedliche Systemplattformen eingesetzt werden, die die grundlegende Online-Funktionalität zur Verfügung stellen.

In der Vielzahl der Online-Spiele stechen die Spiele hervor, die aufgrund ihres wirtschaftlichen Erfolges als Serie, in verschieden Modifikationen oder als Erweiterungen, aufgelegt werden und sich lange in den Verkaufscharts halten. Vertreter dieser Kategorie sind beispielsweise die Grand Theft Auto-Serie oder World of Warcraft mit ihren diversen Erweiterungen.

Datenschutzrechtlich und datensicherheitstechnisch werden die Anforderungen im Bereich der Online-Spiele unter anderem dadurch ständig komplexer, dass die Spieleindustrie immer mehr der insbesondere im Internet erfolgreichen Business-to-Consumer (B2C)-Anwendungen in die Spiele einbaut. So werden in die Online-Spiele Anwendungen wie beispielsweise Shops, In-Game-Advertising, Chats, Nachrichtensysteme und weitere Funktionalität, die man insbesondere aus Sozialen Netzwerken kennt, integriert, um die Spieler an die Produkte zu binden und weitere Umsätze zu generieren.

3.2 Aktuelle Online-Spiele und ihre Datenschutzkomponenten

Der Markt der Online-Spiele bietet eine riesige Anzahl von Spielen. Es ist deshalb nicht möglich, einen annähernd kompletten Überblick über die am Markt befindlichen Online-Spiele zu erstellen. Im Rahmen dieses Vorhabens wurden deshalb einige aktuelle Online-Spiele aufgrund ihrer Aktualität, Bekanntheit oder technischen Neuerung ausgewählt, die im Folgenden aufgeführt werden.

The Legend of Zelda: Phantom Hourglass

Eine erfolgreiche Action-Adventure-Spielserie, die seit geraumer Zeit auch mit Online-Funktionalität ausgestattet ist. Das hier untersuchte Online-Spiel läuft exklusiv auf dem Nintendo DS und dient als Vertreter der Online-Spiele auf mobilen Spielkonsolen.

The Eye of Judgment

Bei diesem Spiel handelt es sich um ein Strategiespiel mit Fantasiethemen für die PlayStation 3, das als Online-Spiel auch eine Kamera in das Spielkonzept integriert hat.

Half-Life 2

Ein weitverbreiteter Ego-Shooter, der auf dem PC und Mac in Verbindung mit der Vertriebsplattform Steam[17], die u. a. weitreichende Kopierschutzvorrichtungen und einige Komponenten von Sozialen Netzwerken bietet, läuft.

Singstar

Singstar ist ein Karaoke-Spiel mit Online-Funktionalität. In Zusammenhang mit der Spielkonsole PlayStation 3 können von den Usern Video- und Audiofiles in die Singstar-Community hochgeladen werden.

Call of Duty 4 – Modern Warfare

Bekannter Ego-Shooter mit Online-Funktionalität. Getestet wurde es auf der Xbox 360 mit Einbindung in das Spielsystem Xbox Live.

World of Warcraft

Eines der bekanntesten MMORPG (Massen-Mehrspieler-Online-Rollenspiele / Multiplayer Online Role-Playing Game) für den PC.

Herr der Ringe Online

Auch Herr der Ringe Online ist ein weit verbreitetes MMORPG für den PC.

Socom – US Navy Seals Freedom Bravo 2

Ego-Shooter für die PlayStation Portable (PSP) mit Online-Audio-Kommunikation mit anderen Spielern.

Final Fantasy XI

Final Fantasy ist eine Rollenspielserie, die ab Version 11 als MMORPG bezeichnet werden kann und das Online-System Xbox Live der Xbox 360 nutzt. Die Besonderheit ist, dass im Gegensatz zu den meisten Spielen, die Xbox Live nutzen, für dieses Spiel nicht die Microsoft Server verwendet werden, sondern der Spieler auf externe Server umgeleitet wird.

Bibi und Tina: Treffpunkt Martinshof

Online-Rollenspiel speziell für Kinder zwischen 7 und 12 Jahren für den PC. Diese Alterklasse unterliegt einem besonderen Schutz und stellt hohe Anforderungen an die Sorgfaltspflicht des Betreibers.

[17] Hersteller und Betreiber ist die Firma Valve Corporation.

Spore

PC-Simulationsspiel, das aufgrund seiner Online-Registrierung und einem DRM-Kopierschutz Empörung in der Spieler-Community ausgelöst hat.

Little Big Planet

„Jump 'n Run“-Online-Spiel für die PlayStation 3, das eine umfangreiche Community-Funktionalität zur Verfügung stellt, über die beispielsweise von den Spielern erstellte Level-designs ausgetauscht und bewertet werden können.

FarmVille

Ein weit verbreitetes Online-Spiel, das in das Soziale Netzwerk Facebook eingebunden ist.

Bei diesen Online-Spielen konnten die in Tabelle 4 / 5 dargestellten Ausprägungen bei den datenschutzrelevanten Modulen festgestellt werden. Die Darstellung erfolgt in abgekürzter Weise, um die Übersichtlichkeit und Vergleichbarkeit zu gewährleisten. Dabei beziehen sich die Angaben nur auf die Relevanz der jeweiligen Funktionalität für das Spiel. Eine Aussage über die Qualität wird damit nicht getroffen.

Tabelle 4: Datenschutzrelevante Funktionen von ausgewählten Online-Spielen (Teil 1)

Online-Spiel / **Modul**	Getestete Plattform	Generelle Vorkehrungen	Vertrieb	Installation und Registrierung	Betrieb und Kontrolle	Bezahlsystem	Kündigung / Spielbeendigung	Spieler-zu-Spieler-Erkennbarkeit	Reputationssystem / Beschwerde-management	Highscoreliste	Ligamodus	Eigenpräsentation des Spielers	Upload	Chat
FarmVille (Facebook)	Browser	X	X	X	X	X	X	X	(X)			X		X
Socom – US Navy Seals Freedom Bravo 2	PSP	X	X	X	X		X	X				X		X
Final Fantasy 11	Xbox 360	X	X	X	X	X	X	X	X			X		X
Bibi und Tina: Treff-punkt Martinshof	PC	X	X	X	X	X	X	X	X			X		X
Spore	PC	X	X	X	X		X	X				X	X	
Little Big Planet	PS 3	X	X	X	X		X	X	X	X		X	X	
Herr der Ringe Online	PC	X	X	X	X	X	X	X	X			X		X
World of Warcraft	PC	X	X	X	X	X	X	X	X			X		X
Call of Duty 4 – Modern Warfare	Xbox 360	X	X	X	X		X	X	X			X		X
Singstar	PS 3	X	X	X	X	X	X	X	X	X		X	X	
Half-Life 2	PC	X	X	X	X	X	X	X		X	(X)	X		X
The Eye of Judgment	PS 3	X	X	X	X		X	X	X	X	X	X		X
The Legend of Zelda: Phantom Hourglass	NDS	X	X	X	X		X	X						

Agenda: X = vorhanden; (X) = teilweise vorhanden

Tabelle 5: Datenschutzrelevante Funktionen von ausgewählten Online-Spielen (Teil 2)

Online-Spiel / Modul	Nachrichtenaustausch	Datenschutzkonfiguration	Datenschutzerklärung	Weiterleitung von Daten an Dritte	In-Game-Advertising	Altersverifikation und Jugendschutz	Suchtprävention	(In-Game-)Shopping	In-Game-Verhaltensanalyse	Webcam / Videoaufzeichnung	Always-Online–Funktionalität (konsolenbezogen)	Mobile-Gaming	Spielen über Internet	Einbindung in Soziale Netzwerke
FarmVille (Facebook)	X	X	X	X	X			X	X				X	X
Socom – US Navy Seals Freedom Bravo 2		X	X	X		X			X			X	X	
Final Fantasy 11	X	X	X	X		X			X				X	
Bibi und Tina: Treff-punkt Martinshof	X	X	X	X		(X)	(X)		X				X	
Spore		X	X	X					X				X	
Little Big Planet	X	X	X	X					X				X	
Herr der Ringe Online	X	X	X	X	X	X		X	X				X	
World of Warcraft	X	X	X	X	X	X		X	X				X	
Call of Duty 4 – Modern Warfare	X	X	X	X		X			X				X	
Singstar	X	X	X	X	X			X	X	X	X		X	
Half-Life 2	X	X	X	X	X	X		X	X				X	
The Eye of Judgment	X	X	X	X				X	X	X	X		X	
The Legend of Zelda: Phantom Hourglass		X	X	X					X			X	X	

Agenda: X = vorhanden; (X) = teilweise vorhanden

3.3 Marktentwicklung und Trends am Beispiel der Spielkonsolen

Online-Spiele locken die Spieler mit einer Vielzahl unterschiedlicher Online-Funktionen, um den Spielspaß und die Spannung in den Spielen zu steigern. Dabei werden die Online-Funktionen in den (Konsolen-) Spielen nicht unwesentlich durch den Funktionsumfang, den die Spielkonsolen mit ihren Spielsystemen zur Verfügung stellen, beeinflusst. Um die Entwicklung der Online-Spiele in Bezug auf den Umfang der Online-Funktionalität zu untersuchen, werden stellvertretend die aus Sicht des Datenschutzes bedeutendsten Spielkonsolen als Basistechnologie für die Spiele untersucht. In einer Zeitachse werden die wichtigsten Neuerungen innerhalb der einzelnen Spielkonsolen und den dazugehörigen Online-Spielsystemen dargestellt.[18]

Xbox / Xbox 360

03/2002 Veröffentlichung Xbox

11/2002 Start Xbox Live
Online-Spielsystem für Xbox/Xbox 360. Es handelt sich hierbei um ein internes Netzwerk, an das die einzelnen Konsolen über das Internet angebunden sind. Funktionen sind unter anderem: Spielersuche und Verbindung, Sprachkommunikation

12/2005 Veröffentlichung Xbox 360

11/2005 Umfassende Erweiterungen von Xbox Live
Neue Funktionen unter anderem:

- Marktplatz (Online-Shop)
- Verbesserte Community-Funktionen
- Gamercard – detailliertes Spielerprofil

10/2006 Erweiterungen von Xbox Live:
Neue Funktionen unter anderem:

- Videochat
- Erweiterter Sprach- und Textnachrichtenversand
- Freundeslisten und Liste mit den 50 zuletzt gespielten Personen
- Gamertag und zugehöriges Profil (Gamercard) können im Internet auf xbox.com außerhalb des Xbox-Netzwerks präsentiert und verwaltet werden
- Reputationssystem

[18] Die Angaben zu den Veröffentlichungen beziehen sich auf Europa.

- Sichtbarkeit, was Freunde im Xbox-Netzwerk gerade spielen und in welchem Level sie sich befinden

11/2009 Anbindung von Facebook und Twitter

11/2009 Video-Dienst für Xbox 360

Angekündigt für 2010

Kinect: Erweiterung der Xbox um Tiefensensorkamera, 3D-Mikrofon und Farbkamera. Dieses ermöglicht eine Ganzkörpersteuerung von Spielen, eine räumliche Erfassung des Aktionsfeldes vor der Spielkonsole und Spielererkennung inkl. Sprachsteuerung.

PlayStation 1 / PlayStation 2 / PlayStation 3

09/1995 Veröffentlichung PlayStation 1

11/2000 Veröffentlichung PlayStation 2
Die Spielkonsole kann mit rudimentären Online-Funktionen (separat zu erwerben) ausgestattet werden.

03/2007 Veröffentlichung PlayStation 3
Start PlayStation Network (PSN)
Online-Spielsystem für PlayStation und PlayStationPortable (PSP). Funktionen sind unter anderem:

- Online-ID: Eindeutiger Username im PlayStation Network
- Detailliertes Spielerprofil
- Online-Mehrspielerfunktion
- PlayStation-Store als Vertriebsplattform für Spiele auf der PlayStation. Die Software wird dabei mitunter durch DRM-Mechanismen[19] geschützt.

06/2008 Start PlayStation Trophies
Es handelt sich um ein Bonussystem und eine Plattform, auf der die Spieler ihre Spielleistungen präsentieren können.

12/2008 Start PlayStation Home (beta)
Mit Home wird das PlayStation Network um eine einer virtuelle Welt erweitert. Home dient dabei als Kommunikationsplattform zwischen den Usern. Der Avatar des Spielers kann auf virtuellen Marktplätzen einkaufen und mit anderen Avata-

[19] Die Abkürzung DRM steht für Digital Rights Management und meint Verfahren mit denen die Nutzung und Verbreitung von digitalen Medien gesteuert wird.

Eine umfassende Darstellung zu Datenschutz und DRM enthält die Studie „Datenschutzverträgliches und nutzerfreundliches Digital Rights Management – Privacy4DRM“ in Zusammenarbeit von Fraunhofer-Institut für Digitale Medientechnologie, Unabhängigen Landeszentrum für Datenschutz und Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau im Auftrag des Bundesministerium für Bildung und Forschung; 2005. Veröffentlicht unter: https://www.datenschutzzentrum.de/drm/.

ren kommunizieren. Eine Reihe zahlungspflichtiger Zusatzinhalte werden angeboten.

10/2009 Start PlayStation Network-Cards
Prepaid-Bezahlsystem für den PlayStation Store

11/2009 PlayStation 3 mit Anbindung von Facebook

11/2009 Erweiterung um einen Videodienst

Wii

12/2006 Veröffentlichung Wii

12/2006 Start WiiConnect24
Online-Spielsystem für die Wii mit ständiger Online-Verbindung[20]. Funktionen sind unter anderem:

- Online-Mehrspielerfunktion
- Wii-Konsolencode zum Nachrichtenaustausch
- E-Mail-Funktion
- Shop-Kanal
- Wii Points Card-Prepaid-Bezahlsystem

02/2007 Umfragen-Channel

04/2007 Integration eines Internetbrowsers

12/2008 WiiSpeak – Sprachkommunikation zwischen mehreren Wii-Konsolen, Hinterlassen von Voice-Nachrichten

MobileDevice

PSP (PlayStation Portable)

09/2005 Veröffentlichung PSP-1000

05/2007 Zubehör: Kamera für PSP (Go!Cam)

10/2008 PSP-3000 mit integriertem Mikrofon

10/2009 Veröffentlichung PSP Go
Spiele können nur noch online im PlayStation Store gekauft und runtergeladen werden

10/2009 PlayStation Network-Cards-Prepaid-Bezahlsystem

[20] Die Wii ist auch im Standby-Modus in Verbindung mit den Servern des Betreibers und empfängt Updates und Nachrichten.

iPhone, iPod, iPad (iOS)

11/2007 Veröffentlichung iPhone

07/2008 Eröffnung App Store: Online-Verkauf von Software und Spielen für iPhone und iPod touch.

01/2010 Ankündigung iPad

Abbildung 3: Entwicklung Spielkonsolen im Hinblick auf Online-Funktionalitäten

Die Darstellung der Entwicklung der Spielkonsolen mit ihren Grundfunktionen lässt erkennen, dass das Konzept der Spielkonsolen vom Spielgerät nur für die Familie inzwischen überholt ist. Die Spielkonsolen bieten eine Reihe von Online-Funktionen und vereinen diese zu einem Gesamtkonzept. Dass Spieler online zusammen ein Spiel spielen können, gehört zu der Grundausstattung einer Spielkonsole. Mit modernen Spielkonsolen können die Spiele im Online-Shop eingekauft, mit anderen Spielern gechattet, Text- und Videonachrichten ausgetauscht, die Spielerprofile mit zusätzlichen Informationen ergänzt und Spielaktivitäten und -ergebnisse präsentiert werden. Der neuste Trend geht dahin, dass Spielkonsolen sich mit den bestehenden Sozialen Netzwerken wie Facebook, StudiVZ oder Twitter verbinden. Bestand bis vor Kurzem noch ein Medienbruch zwischen Online-Spielen und Sozialen Netzwerken, so wachsen die verschiedenen Medien immer weiter zusammen. Durch diese Entwicklungen steigen auch die Datenschutzanforderungen an die Hersteller und Betreiber, aber auch die Spieler sollten sich möglicher Risiken durch diese Entwicklung bewusst sein. Haben Nutzer bislang mindestens zwei getrennt von einander existierende digitale Identitäten gepflegt, nämlich die des Spielers und die in einem Sozialen Netzwerk, so können diese Informationen nunmehr verkettet werden. Als Spieler präsentiert man der Öffentlichkeit damit ein breiter gefächertes Profil über einen selbst.

Der gleiche Trend ist auch bei den mobilen Geräten wie dem iPhone zu erkennen. Die Apps[21], unter denen auch zahlreiche Online-Spiele zu finden sind, drängen in die persönlichen sozialen Kontaktinformationen. Jede Applikation auf dem iPhone hat Zugriff u. a. auf E-Mail-Accounts und das Adressbuch, das auf dem Telefon gespeichert ist.

Aus Datenschutzsicht sind die angesprochenen Entwicklungen im Bereich der Online-Spiele kritisch zu begleiten. Es steht zu erwarten, dass der Umfang der Funktionalität bei der Einbindung von Sozialen Netzwerken in die Online-Dienste der Spielkonsolen weiter wachsen wird.

3.4 Zukünftige Entwicklungen

Aus den aktuellen Entwicklungen auf dem Spielemarkt lassen sich einige Trends erkennen, die in den kommenden Monaten und Jahren zu besonderen Datenschutzproblemen führen können:

Verarbeitung von Gesundheitsdaten

Spiele wie Wii Fit[22] und Your Shape[23] für die Nintendo Wii oder auch Laufrhythmus DS für den Nintendo DS zeigen die Entwicklung auf, dass Spiele mit Effekten auf das Wohlbefin-

[21] Apps ist die Kurzform von „Applications“ (oder „Applikationen“, „Anwendungen“). Unter Applications sind die verschiedensten Software-Produkte, Tools oder Online-Spiele zusammengefasst.

[22] Fitness Spiel mit dem Wii Balance Board, dass zur Steuerung dient, aber beispielsweise mit integrierter Waage auch das Gewicht des Spielers ermittelt.

[23] Fitness Spiel mit einer Kamera und Kamera-Tracking-Technologie zur Überprüfung der Fitnessübungen.

den, die Fitness und Gesundheit auf Interesse bei den Spielern stoßen. Bisher sind die Online-Funktionen dieser Spiele gering ausgeprägt. Jedoch ist anzunehmen, dass das Interesse der Spieler, sich auch in diesen Bereichen zu vergleichen, bedient werden wird. So hat Nike mit Nike+[24] für den iPod ein System etabliert, mit dem Zeiten und Strecken beim Jogging online verglichen werden können. Diese Daten werden auf Wunsch über eine Webseite veröffentlicht und sind damit für jedermann einsehbar.

Aus Datenschutzsicht handelt es sich hierbei teilweise um Gesundheitsdaten und damit um besondere Arten von personenbezogenen Daten gemäß § 3 Abs. 9 BDSG. Für diese gelten strengere Verarbeitungsbedingungen.

Entwicklung hin zum reinen Online-Vertrieb von Spielen

Sowohl Microsoft mit Xbox Live als auch Sony mit dem PlayStation Network (PSN) bieten zahlreiche Spiele zum Online-Kauf an. Auch Nintendo bietet inzwischen Wii-Spiele und Spiele für den NDS online an. Im Oktober 2009 ist die PSP Go von Sony erschienen, die ausschließlich online erworbene Spiele verarbeiten kann. Das iPhone und iPad waren von vornherein darauf ausgelegt, nur Spiele über den App Store abzurufen.

Der Online-Vertrieb hat für die Hersteller bzw. Publisher den Vorteil, dass sie die Kontrolle über die vertriebenen Spiele behalten. Ein Gebrauchtmarkt ist praktisch ausgeschlossen. Spiele können von den Herstellern im Nachhinein noch verändert oder sogar gelöscht werden. Kopierschutzvorrichtungen lassen sich so gestalten, dass die Nutzung eines Spiels an eine bestimmte Konsole gebunden ist und ein Konsolenwechsel überwacht werden kann.

Aus Datenschutzsicht problematisch an dieser Entwicklung ist, dass mit der Kontrolle der Hersteller über die Spiele auch die Überwachung des Spielers verbunden sein kann. Es wird kaum noch möglich sein, das Spielen bestimmter Spiele komplett anonym zu gestalten. Für die Online-Vertriebswege ist es bei den bestehenden Systemen in der Regel notwendig, sich zu registrieren. Eine anonyme Nutzung ist nur bedingt möglich, auch wenn Nutzer teilweise (z. B. im PSN) Prepaid-Karten verwenden können. Die Herausforderung wird darin bestehen, dem durchaus verständlichen Interesse der Hersteller und Verkäufer von Spielen an einem wirksamen Kopierschutz zu entsprechen und gleichzeitig eine vollständig anonyme Nutzung der Spiele zu ermöglichen.

Ausbau des In-Game-Advertisings hin zur Analyse von Interessen und Verhaltensmustern

In-Game-Advertising steht noch am Anfang seiner Entwicklung. Die Entwicklung bei anderen Telemedien, insbesondere den normalen Webseiten, hin zu ausgeklügelten Targeting-Lösungen, zeigt, dass ein Interesse daran besteht, zielgruppengerechte Werbung einzublenden und Streuverluste gering zu halten. Bei Online-Spielen lassen sich insbesondere aus der Art der gespielten Spiele und aus dem Spielverhalten Aussagen über den Spieler treffen.

[24] Aus dem Nike Sportschuh werden beim Laufen Sensordaten zum iPod übertragen. Im iPod werden die Trainingsdaten ausgewertet und auf Wunsch dem Sportler angesagt.

Hinzu kommen Daten, die der Betreiber durch die Anmeldung des Spieler und / oder über sein Soziales Netzwerk erhält. Mit diesen Daten können über statistische Modelle Vermutungen über die Interessen des Spielers aufgestellt werden, die sich dann von Werbetreibenden zur gezielten Ansprache nutzen lassen.

Aus Datenschutzsicht darf die Entwicklung nicht dazu führen, dass für Werbetreibende der Spieler zum gläsernen Nutzer wird. Einige Targeting-Anbieter haben dieses für den Bereich der Werbung auf Webseiten schon erkannt und haben ihre datenschutzkonforme Realisierung durch Datenschutz-Gütesiegel bestätigen lassen[25]. Sie zeigen, dass eine gezielte Werbeansprache auch datenschutzgerecht möglich ist, indem ein Rückschluss auf die konkrete Person mittels Einsatz von Pseudonymen und Anonymisierungsdiensten so weit wie möglich ausgeschlossen wird.

Integration von Online-Spielen in Soziale Netzwerke

Die jüngst großen Erfolge von Spielen wie FarmVille oder auch Mafia Wars in Facebook weisen darauf hin, dass die Einbindung von Spielen in Sozialen Netzwerken zunehmen wird. Im Gegenzug entwickeln sich die Spielsysteme selbst mehr und mehr zu eigenen Sozialen Netzwerken und binden inzwischen Dienste wie Twitter oder Facebook aktiv ein. Die Grenzen zwischen Online-Spielen und Sozialen Netzwerken verschwimmen. Damit droht die Gefahr, dass bei der Einbindung von Spielen der Überblick verloren geht, wo jeweils Bestandsdaten, Nutzungsdaten und Kommunikationsinhalte zu welchen Zwecken verarbeitet und von wem diese eingesehen werden können.

Aktuelle Entwicklungen zeigen jedoch, dass diesem Trend der Intransparenz von einigen Betreibern der entsprechenden Plattformen durch datenschutzfreundlichere und nachvollziehbare Techniken entgegen gewirkt wird. So hat StudiVZ im Dezember 2009 die Einbindung von externen Diensten so realisiert, dass der Nutzer im Vorfeld entscheiden kann, welche Daten an den Dienst übermittelt werden[26]. Dabei kann er die Daten meist sogar noch individuell ändern. Auch später hat er die Möglichkeit, einzusehen, auf welche Daten die Applikation Zugriff hat, und kann diese Zugriffsrechte der Applikation jederzeit wieder entziehen.

Erfassung der Physiognomie eines Menschen

Seit dem großen Erfolg der Wii von Nintendo sind auch Microsoft und Sony dabei, Techniken zu entwickeln, die weggehen von der Eingabe mit dem Joystick bzw. Pad hin zu Steuerungen mit dem gesamten Körper. Insbesondere Kinect (ehemals Projekt Natal)[27] von Microsoft deutet darauf hin, dass mittels mehrerer Kameras und Sensoren zukünftig ganze Räume und

[25] Z. B. die Hersteller nugg.ad, wunderloop, Group M oder 1&1. Die Kurzgutachten können auf der Webseite des ULD abgerufen werden unter: https://www.datenschutzzentrum.de/guetesiegel/register.htm.

[26] Pressemitteilung der VZnet Netzwerke Ltd. vom 07.12.2009, VZ-Netzwerke präsentieren einmaliges OpenSocial konzept mit umfassender Datenschutzlösung, Abrufbar unter: http://static.pe.studivz.net/media/de/pm/091207.pdf.

[27] Markteinführung für November 2010 angekündigt.

Personen erfasst werden sollen und dass diese Technik sogar Personen wiedererkennen kann.

Aus Datenschutzsicht muss darauf geachtet werden, dass diese Funktionen nicht zu einer weitergehenden Überwachung der Hausbewohner führt, auf die beispielsweise der Betreiber des Systems Zugriff hat.

Spiele mit Erfassung von Positionsdaten

Durch die zunehmende Verbreitung von mobilen Spielgeräten bzw. zum Spielen geeigneten Handys wie dem iPhone werden auch Spiele möglich, die die konkrete Umgebung des Spielers mit einbinden. Spiele wie Mister X Mobile, FastFood-Challenge[28] oder auch GPS-Mission[29] erlauben schon heute mit entsprechenden Geräten Outdoor-Spiele, bei denen Positionsdaten ausgetauscht werden, um z. B. die Mitspieler zu fangen.

Aus Datenschutzsicht ist die Erfassung der Positionen der Spieler durch den Betreiber des Spiels auf das Notwendige zu reduzieren und muss transparent sein. Das Telekommunikationsgesetz beinhaltet Vorgaben, wie Positionsdaten verarbeitet werden dürfen, woran sich auch die Betreiber entsprechender Spiele halten müssen. Insbesondere muss die Verarbeitung dieser Daten auf die Erbringung des Spiels beschränkt bleiben. Nach Beendigung des Spiels ist diese Funktion wieder zu deaktivieren.

[28] FastFood-Challenge ist eine GPS Multiplayer Spiel, dass eine vorher definierte Outdoorspielfläche hat auf der ein Mitspieler zu fangen sind. Weitere Informationen unter: http://www.fastfoot.mobi/.

[29] GPS-Mission ist ein GPS-Spiel, in dem der Spieler bestimmte Missionen (Aufgaben) Outdoor erfüllen muss. Weitere Informationen unter: http://gpsmission.com/.

4 Datenerhebung in Online-Spielen

Ausgangspunkt der Studie sind die bei Online-Spielen anfallenden personenbezogenen Daten. Im Folgenden werden die Datenerhebungen, -verarbeitungen und -nutzungen anhand der verschiedenen Phasen, in die Spieler, Publisher und Betreiber eingebunden sind, erläutert. Diese Auflistung ermöglicht es, die anfallenden personenbezogenen Daten zu identifizieren und die datenschutzrechtlichen Aspekte für die aufgeführten Funktionen herauszuarbeiten.

Personenbezogene Daten von Spielern werden vor allem durch den Publisher, den Betreiber des Spiels und durch Dritte, die in den Spielbetrieb bzw. die damit zusammenhängenden Funktionalitäten eingebunden sind, in unterschiedlichen Phasen des Online-Spiels erhoben, verarbeitet und genutzt. Dies geschieht unter anderem für den Vertrieb, die Installation, den Spielbetrieb selbst und die Bezahlung/Abrechnung. Die für die einzelnen Phasen der Spielnutzung erforderlichen bzw. anfallenden personenbezogenen Daten unterscheiden sich von Spiel zu Spiel. Einige Online-Spiele werden kostenlos zur Verfügung gestellt; Abrechnungsdaten sind für diese Spiele nicht erforderlich bzw. allenfalls gegenüber Werbepartnern relevant. Andere Online-Spiele beinhalten zusätzliche Optionen, wie Chat- und Videomöglichkeiten, Highscorelisten, Bewertungen der jeweiligen Spieler usw. Für diese Optionen sind zusätzliche personenbezogene Daten der Spieler erforderlich. Insoweit werden die gefundenen Funktionalitäten in den Leitfaden aufgenommen.[30] Dies soll anhand der Spielfunktionen den Spielern, Betreibern, Publishern und Herstellern bzw. Entwicklern eine modulare Einschätzung der spezifischen datenschutzrechtlichen Probleme für die einzelnen Spiele ermöglichen.

Aufgrund der Vielzahl der unterschiedlichen Online-Spiele und der dort anfallenden personenbezogenen Daten kann die folgende Auflistung nur eine kurze Einführung in die Problematik geben. Eine abschließende Auflistung ist aufgrund der dynamischen Entwicklung von Online-Spiele nicht möglich.

4.1 Datenerhebung beim Vertrieb von Online-Spielen

Beim Vertrieb von Online-Spielen fallen die personenbezogenen Daten in aller Regel beim Publisher an. Der Vertrieb erfolgt entweder auf klassische Art und Weise über Händler bzw. Geschäfte oder online. Erfolgt der Vertrieb eines Online-Spiels im Geschäft, so werden vom Verkäufer in der Regel keine personenbezogenen Daten erhoben. Bezahlt der Spieler nicht bar, werden üblicherweise für den Bezahlvorgang Kreditkarten- bzw. EC-Kartendaten erhoben. Wird bei der Bezahlung eine Kundenkarte eingesetzt, fallen auch hier personenbezoge-

[30] Siehe dazu Kapitel 9.

ne Daten, wie Name, Adresse, gegebenenfalls Geburtsdatum oder Telefonnummer, an. Diese Daten werden dann mit den Daten aus dem Kauf, Kaufdatum, Kaufgegenstand und Kaufpreis ergänzt.

Zusätzlich werden bei Online-Käufen und altersbeschränkten Online-Spielen Altersverifikationen vorgenommen. Neben der Erhebung des Geburtsdatums wird in diesen Fällen oft ein PostIdent-Verfahren durchgeführt, in welchem sich die Online-Spieler ausweisen müssen und in dem die jeweiligen Personalausweisnummern erhoben werden. Einige Publisher/Betreiber gehen sogar soweit, eine vollständige Kopie des Personalausweises / Passes zu verlangen.

4.2 Datenerhebung bei der Installation und der Registrierung von Online-Spielen

Im Rahmen der Installation und Registrierung der Online-Spiele werden oft u. a. der Name des Spielers, seine Anschrift, seine IP-Adresse, E-Mail-Adresse und eventuell das Geburtsdatum / Alter erhoben. Diese Daten werden für die Erstellung eines Spielerprofils verarbeitet. In vielen Fällen werden bei der Installation eines Spiels auch Cookies auf dem PC des Spielers hinterlassen und Daten über den PC, etwa installierte Programme und Hardwareinformationen, erhoben. Dies kann für die Spielversion und das Spielverhalten erforderlich sein. Ob es sich bei den genannten Daten um personenbezogene Daten handelt, ist teilweise umstritten und bedarf im weiteren Verlauf der Studie einer umfangreicheren Darstellung.[31]

4.3 Datenerhebung während des Betriebs von Online-Spielen

Während des Spielbetriebs werden weitere personenbezogene Daten erhoben, verarbeitet und genutzt. Dies umfasst vor allem Daten zu seinem Spielverhalten (z. B. Reaktionszeiten, Spielsystem, Spielverlauf, Spielverhalten, gespielten Spiele und Level), kann jedoch auch die Kommunikation der Spieler untereinander und Clickstream-Daten umfassen. Dies erfolgt entweder in Verbindung zum Echtnamen des Spielers oder unter einem Pseudonym.

4.4 Datenerhebung bei der Abrechnung und Bezahlung im Rahmen von Online-Spielen

Kostenpflichtige Online-Spiele und kostenpflichtige Zusatzoptionen werden in der Regel online per Kreditkarte / Paypal oder per Überweisung bezahlt. In diesen Fällen können Kontodaten des Spielers erhoben, verarbeitet und genutzt. Bei einigen Online-Spielen ist es auch möglich, mit Prepaid-Karten zu bezahlen, so dass in diesen Fällen für die Abrechnung keine personenbezogenen Daten erforderlich sind.

[31] Siehe dazu Kapitel 8.2.

4.5 Datennutzung in Sozialen Netzwerken

Weitere Nutzungen personenbezogener Daten ergeben sich in Sozialen Netzwerken. So sind in den vergangenen Jahren Online-Spiele in Soziale Netzwerke wie Facebook, StudiVZ und SchülerVZ integriert worden, die es möglich machen, die im Rahmen des Sozialen Netzwerks erhobenen Daten in das jeweilige Spiel zu integrieren und mit dort erhobenen Daten zu verketten bzw. zu kombinieren. Diese neue Form der Datenverkettung ist insoweit datenschutzrelevant, als die miteinander verketteten Daten zu anderen als den Spielzwecken erhoben wurden und insoweit eine Zweckänderung eintritt, die einer rechtlichen Grundlage bedarf. Auch können hier personenbezogene Daten Dritter hinzukommen (z. B. von „Freunden“ im Sozialen Netzwerk), für die keine Einwilligung vorliegt.

4.6 Besonderheiten: Zufällig anfallende Daten

In den aufgeführten Phasen fallen nicht nur die beim Betroffenen angeforderten personenbezogenen Daten an, sondern zusätzliche personenbezogene Daten, welche ohne Aufforderung gewonnen werden. Dies sind personenbezogene Daten, über die sich der Online-Spieler in den meisten Fällen nicht bewusst ist, und Daten, die der Online-Spieler selbst unaufgefordert von sich preisgibt. Zufällig anfallende Daten sind nicht vom Begriff der „Erhebung“ umfasst.[32] Solange diese nicht verarbeitet oder genutzt werden, finden die Datenschutzbestimmungen auf diese insoweit keine Anwendung.[33] Im Hinblick auf den Schutzgedanken der Datensparsamkeit sind die Verantwortlichen jedoch verpflichtet, die Zahl der zufällig anfallenden Daten so gering wie möglich zu halten und diese nach dem Anfall umgehend zu löschen.

[32] Siehe dazu Kapitel 5.2.2.

[33] Heckmann, in: juris PK-Internetrecht, Kapitel 1.12, Rn. 36.

5 Anwendbare Datenschutzbestimmungen

Einen rechtlichen Rahmen speziell ausgelegt auf Online-Spiele gibt es nicht. Vielmehr sind alle diejenigen Rechtsnormen zu berücksichtigen, die für die einzelnen bei Online-Spielen auftretenden Rechtsprobleme Regelungen enthalten. Hinsichtlich der in der Studie zu beurteilenden Rechtsprobleme wird im Folgenden der datenschutzrechtliche Ordnungsrahmen skizziert.

Da sowohl die verschiedenen Spieler von Online-Spielen als auch die Betreiber prinzipiell ortsunabhängig bei der Nutzung und dem Angebot von Online-Spielen sind, stellt sich in diesem Zusammenhang die Frage nach dem anwendbaren Recht. Dies bezieht sich einmal auf die zur Anwendung kommende Rechtsordnung, also internationale Regelungen, das Recht der Europäischen Union oder nationale Rechtsordnungen, und auf einer zweiten Ebene auf die jeweils inhaltlich anwendbaren Datenschutzbestimmungen. So bestehen datenschutzrechtlich relevante Normen allgemein für personenbezogene Daten, personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien und personenbezogene Daten im Zusammenhang mit der Übermittlung von Telekommunikationsdienstleistungen.

Insoweit sind in einer ersten Prüfung die anwendbaren Rechtsordnungen und deren Datenschutzbestimmungen aufzuführen (siehe Abschnitt 5.1), sodann ist zu erörtern, in welchen Fällen welche Rechtsordnung maßgeblich ist (siehe Abschnitt 5.2), und in einem dritten Schritt sind die jeweils konkret inhaltlich anwendbaren Datenschutzregelung innerhalb der anwendbaren Rechtsordnung zu identifizieren (siehe Abschnitt 5.3).

5.1 „Örtlich“ anwendbare Datenschutzbestimmungen

Die Möglichkeiten, Online-Spiele grenzüberschreitend zu nutzen und anzubieten, führt dazu, dass unterschiedliche Rechtsordnungen auf einen konkreten Sachverhalt Anwendung finden könnten: So haben Publisher und Betreiber von Online-Spielen ihren Hauptsitz in unterschiedlichsten Staaten; die Server, auf denen die Online-Spiele gespielt werden, können weltweit auf andere Staaten verteilt stehen, und oft ist es Zufall, welcher Server genutzt wird. Der Spieler selbst hat auf den Standort des Servers bzw. die Entscheidung, welchen Server er nutzen möchte, selten Einfluss. Auch die Spieler von Online-Spielen können von allen möglichen Staaten der Erde aus agieren. Insoweit ist zu ermitteln, welches örtliche Datenschutzrecht für die jeweiligen Sachverhalte Anwendung findet.

5.1.1 Internationales Recht

Auf internationaler weltweiter Ebene lassen sich keine verbindlichen Regelungen zum Da-

tenschutz finden. Die OECD hat 1980 die „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“ entwickelt.[34] Diese Leitlinien stellen jedoch kein verbindliches Völkerrecht dar, sondern sind ausschließlich dazu gedacht, einen Hinweis für die Entwicklung nationaler Datenschutzgesetze zu geben. Sie können insoweit für die Studie selbst keinen Bewertungsmaßstab setzen. Ebenfalls ausschließlich empfehlenden Charakter haben die „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien“ der Generalversammlung der Vereinten Nationen (UN) vom Dezember 1990.[35] Es handelt sich auch hier nicht um bindendes Völkerrecht.

Weiterhin ist international Art. 8 der Europäischen Menschenrechtskonvention (EMRK) zu berücksichtigen. Diese Regelung ist regional begrenzt auf die Mitgliedstaaten des Europarates. Sie enthält keine speziellen Regelungen zum Datenschutz und hat im Ergebnis einen reinen Schutzcharakter, da es sich um ein Grundrecht handelt.

Neben diesen internationalen Regelungen zum Datenschutz ist das so genannte „Safe Harbor-Abkommen“ zu berücksichtigen. Dieses Abkommen wurde zwischen den USA und der Europäischen Union abgeschlossen. Inhaltlich stellt es einzelne Datenschutzprinzipien auf, die teilweise ein ähnlich hohes Schutzniveau wie die EG-Datenschutzrichtlinie aufweisen. US-Unternehmen, welche sich den Prinzipien des Abkommens unterworfen haben und von der Europäischen Kommission anerkannt wurden, sollen ein den EU-Bestimmungen entsprechendes Datenschutzniveau gewährleisten. Diese US-Unternehmen sind in einer für alle EU-Bürger einsehbaren Liste des US-Handelsministeriums aufgeführt.[36]

5.1.2 Europarecht

Publisher bzw. Betreiber von Online-Spielen müssen, soweit sie ihren Hauptsitz in der Europäischen Union haben, das Recht der Europäischen Union beachten. Im Gegensatz zu den bereits aufgeführten Rechtsinstrumenten sind die Datenschutzbestimmungen der Europäischen Union für die Mitgliedstaaten der Europäischen Union bindend. Im Bereich des Datenschutzes sind seit dem 1. Dezember 2009 in Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Art. 8 EU-Grundrechtecharta jeweils Grundrechte zum Schutz der personenbezogenen Daten verankert. Dabei ist Art. 16 AEUV in erster Linie eine Kompetenzregelung zugunsten der Europäischen Union und Art. 8 EU-Grundrechtecharta das eigentliche Grundrecht auf Datenschutz mit entsprechenden Schrankenregelungen in Art. 52 Abs. 1 EU-Grundrechtecharta.

Beide Regelungen sind vom Wortlaut her identisch. Die Rechtsprechung des Europäischen Gerichtshofes hat bereits ohne die Verbindlichkeit des Art. 8 EU-Grundrechtecharta ein europäisches Grundrecht auf Datenschutz anerkannt. Danach werden privatrechtliche Sach-

[34] OECD Declaration on Transborder Data Flows, The OECD Observer, Nr. 135.

[35] UN Resolution 45/95, http://www.un.org/documents/ga/res/45/a45r095.htm.

[36] https://www.export.gov/safehrbr/list.aspx.

verhalte von dem europäischen Grundrecht auf Datenschutz erfasst.[37] Zusätzlich ist über Art. 6 Abs. 3 des Vertrages der Europäischen Union (EUV) auch Art. 8 der Europäischen Menschenrechtskonvention (EMRK) zu berücksichtigen, da die Europäische Union die Grundrechte, wie sie in der EMRK festgelegt werden, achtet.

Einfachgesetzlich ergibt sich für das Gebiet der Europäischen Union ein Mindeststandard im Datenschutzrecht aus den Richtlinien des Europäischen Parlaments und Rats 95/46/EG aus dem Jahre 1995[38] (allgemeine Datenschutzrichtlinie) und 2002/58/EG aus dem Jahr 2002[39] für die Bereiche Telemedien und Telekommunikation. Für Online-Spiele zusätzlich von Bedeutung sind die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten[40] und die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[41]. Beide Richtlinien befassen sich zwar nicht vordergründig mit Datenschutz. Sie beinhalten jedoch Regelungen zur Kommunikation im Internet.

Richtlinien selbst erzeugen keine direkte innerstaatliche Wirkung in den Mitgliedstaaten der Europäischen Union. Richtlinien sind gemäß Art. 288 Abs. 3 AEUV (Art. 249 Abs. 3 EGV) an die Mitgliedstaaten der Europäischen Union gerichtet und nur hinsichtlich des zu erreichenden Ziels verbindlich. Sie sind von den einzelnen Mitgliedstaaten in nationales Recht umzusetzen. Die Mittel und die Form der Umsetzung können die Mitgliedstaaten frei wählen. Insoweit ist nur das umgesetzte nationale Recht verbindlich und für die Publisher und Betreiber von Online-Spielen von Bedeutung.

Für diese Untersuchung sind die Richtlinien jedoch insoweit von Bedeutung, als sie in allen Mitgliedstaaten der Europäischen Union in nationales Recht umgesetzt wurden und das gesamte mitgliedstaatliche Recht im Bereich des Datenschutzes und der Telekommunikation harmonisiert wurde. Hierdurch wurde ein europaweit einheitliches Datenschutzniveau geschaffen, was primär den grenzübergreifenden Datenverkehr im Binnenmarkt fördern soll. Insoweit können die Richtlinien, trotz der fehlenden unmittelbaren Wirkung, zur Begründung

---

[37] EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971, Tz. 24; EuGH, Rs. C-275/06 (Promusicae), Slg. 2008, S. I-271, Tz. 57.

[38] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABL. EG Nr. L 281 vom 23.11.1995, S. 31-50.

[39] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 vom 31.07.2002, S. 37-47.

[40] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EG Nr. L 105 vom 13.04.2006, S. 54-63.

[41] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG Nr. L 24 vom 30.01.1998, S. 1-8.

eines Mindeststandards und zur Überprüfung der datenschutzrechtlichen Vorgaben für Online-Spiele herangezogen werden.

Die EG-Datenschutzrichtlinie 95/46/EG schafft einen allgemeinen Rechtsrahmen zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG hingegen strebt ein einheitliches Rechtsregime für alle Formen elektronischer Kommunikation an. Sie erfasst sowohl Telemedien- als auch Telekommunikationsdienste.

Auszuschließen ist aus der hier geführten Betrachtung trotz ihrer Nähe zu Webanbietern die Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"). Diese Richtlinie umfasst gemäß Satz 2 des 18. Erwägungsgrunds alle mit dem Online-Verkauf von Waren verbundenen Tätigkeiten, bei den Online-Spielen handelt es sich aber in der Regel gerade nicht um Waren, sondern um Dienstleistungen. Auch die Richtlinie 2007/65/EG über audiovisuelle Mediendienste für die Bestimmung des jeweils geltenden Rechts bleibt in dieser Studie außen vor, da sie keine Datenschutzbestimmungen enthält. Gemäß Erwägungsgrund 18 der Richtlinie sind Online-Spiele auch ausdrücklich nicht vom Anwendungsbereich der Richtlinie umfasst.[42] Hintergrund dieser Entscheidung ist der Hauptzweck von Online-Spielen. Online-Spiele sind nicht vorrangig audiovisuelle Medien, sondern vielmehr Dienstleistungsangebote im Rahmen der Unterhaltung. Audiovisuelle Inhalte werden nur als Nebenerscheinungen transportiert.

5.1.3 Deutsche Datenschutzbestimmungen

Grundlage des deutschen Datenschutzrechts ist das Verfassungsrecht. Dem deutschen Gesetzgeber ist durch das Grundgesetz ein Schutzauftrag für die informationelle Selbstbestimmung der in Deutschland ansässigen Personen aufgegeben worden.[43] Dieser Auftrag ist durch die Rechtsprechung des Bundesverfassungsgerichts in den letzten Jahren bestätigt worden.[44] Teilweise wird sogar ein „Kommunikationsgrundrecht" der Bürger angenommen.[45] Die personenbezogenen Daten der Bürger werden als besonders schützenswert angesehen. In seiner inhaltlichen Ausprägung gibt dieses Recht dem Grundrechtsträger die Möglichkeit, grundsätzlich selbst über die Erhebung und Verwendung seiner personenbeziehbaren Daten zu entscheiden. Dabei handelt es sich um einen Schutz, der auch in den Fällen angestrebt wird, in denen eine Verarbeitung von Daten gar nicht oder nicht hauptsächlich in Deutsch-

---

42 Richtlinie 2007/65/EG des Europäischen Parlaments und des Rates vom 11.12.2007 zur Änderung der Richtlinie 89/552/EWG des Rates zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG Nr. L 332 vom 18.12.2007, S. 27 (29).

43 BVerfGE 65, 1 (42).

44 BVerfG NJW 2008, 822.

45 Leisner, in: NJW 2008, 2902 ff.

land stattfindet. Die Grundrechte können aber jeweils durch ausdrückliche oder verfassungsimmanente Schranken beschränkt werden. Zu berücksichtigen sind dabei in erster Linie Grundrechte Dritter.

Spezialgesetzliche Regelungen zum Datenschutz finden sich unter anderem im Bundesdatenschutzgesetz (BDSG), dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG). Für den Bereich der Online-Spiele als Telemedien oder sonstige Dienste sind vorrangig die Bestimmungen des BDSG und des TMG anzuwenden. Das BDSG und die datenschutzrechtlichen Bestimmungen im TMG sind Folgen der Umsetzung der aufgeführten europäischen Datenschutzrichtlinien. Soweit Telekommunikationsdienste wie E-Mail angeboten werden, kommt das TKG zur Anwendung.

Für datenschutzrechtliche Belange in Angeboten privatwirtschaftlicher Unternehmen ist unabhängig von der Form des Angebotes neben den allgemeinen Regelungen insbesondere der dritte Abschnitt des BDSG (§§ 27 ff. BDSG) einschlägig. Dies gilt entsprechend auch für das Angebot von Online-Spielen sowie für deren Publisher und Betreiber.

Der Anwendungsbereich der Datenschutzbestimmungen ist eröffnet, wenn personenbezogene Daten durch öffentliche oder nicht-öffentliche Stellen erhoben, verarbeitet oder genutzt werden (§ 1 BDSG und § 1 TMG). Ausgeschlossen sind Datenerhebungen, -nutzungen und -verarbeitungen, welche ausschließlich für persönliche und familiäre Tätigkeiten erfolgen (§ 1 Abs. 2 Nr. 3 BDSG). Der Gesetzgeber will damit in Umsetzung des Art. 3 Abs. 2 Spiegelstr. 3 EG-Datenschutzrichtlinie klarstellen, dass lediglich solche Erhebungen, Verarbeitungen oder Nutzungen der personenbezogenen Daten in den Anwendungsbereich der Datenschutzbestimmungen fallen, die kommerzielle Verarbeitungen, mithin geschäftsmäßig für berufliche oder gewerbliche Zwecke erfolgende Verarbeitungen, zum Gegenstand haben. Im Fall einer rein privaten Verarbeitung ist das BDSG daher nicht anwendbar.[46] Etwas anderes gilt, wenn die Tätigkeit aus dem persönlich-familiären Bereich herausragt, so z. B. bei Webangeboten, auch wenn diese an und für sich von privater Natur sind.[47]

Voraussetzung für die Anwendung der Datenschutzbestimmungen ist demnach das Vorliegen eines personenbezogenen Datums. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG alle Informationen über eine bestimmte oder bestimmbare natürliche Person.[48]

Neben den allgemeinen datenschutzrechtlichen Bestimmungen des BDSG gelten für die Anbieter von Telemedien die speziellen datenschutzrechtlichen Vorgaben der §§ 11-15 TMG. Telemedien sind gemäß § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht die Tatbestandsmerkmale eines Telekommunikations-

---

[46] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1 Rn. 116.

[47] EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971, Tz. 46 f.; Weichert, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 1 Rn. 9.

[48] Siehe dazu Kapitel 8.2.

dienstes nach § 3 Nr. 24 TKG oder des Rundfunks nach § 2 Rundfunkstaatsvertrag erfüllen. Insoweit werden Online-Spiele in der Mehrzahl als Telemedien zu charakterisieren sein.[49] Der Begriff der Telemedien ist zwar weder im TMG noch im TKG legal definiert. Aus § 1 Abs. 1 TMG ergibt sich jedoch, dass sie alle elektronischen Informations- und Kommunikationsdienste erfassen sollen, „soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk sind“. Folgt man der Definition des Teledienstegesetzes (TDG) als Vorgänger des TMG, so waren von § 2 Abs. 1 TDG nur solche Dienste erfasst, die mittels Telekommunikation übermittelt wurden.[50] Für Spiele, welche auf Datenträger verkörpert sind, ist das TMG zwar demnach zunächst nicht anwendbar. Da der Begriff Online-Spiele eine Übermittlung der Daten mittels Telekommunikation voraussetzt, sind jedoch zumindest alle Online-Spiele, welche im Ergebnis auch Daten mittels Telekommunikation übertragen, als Telemedien zu qualifizieren. Insoweit findet neben dem BDSG auch das TMG Anwendung.

Datenschutzrechtlich relevant sind für Online-Spiele die Regelungen des vierten Abschnitts des TMG. § 11 TMG legt den Anwendungsbereich der datenschutzrechtlichen Bestimmungen des TMG fest, § 12 TMG enthält die allgemeinen Grundsätze, die Anbieter von Telemedien bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten berücksichtigen müssen. § 13 TMG bestimmt die wesentlichen Informationsverpflichtungen eines Telemedienanbieters, und die §§ 14 und 15 TMG enthalten die Voraussetzungen für die Erhebung, Nutzung und Verarbeitung personenbezogener Daten ohne die Einwilligung des Betroffenen.

Gemäß § 11 TMG finden die Datenschutzbestimmungen des TMG auf Dienst- und Arbeitsverhältnisse und die Steuerung von Arbeits- und Geschäftsprozessen keine Anwendung. Demnach gilt im Umkehrschluss aber auch, dass die §§ 11 ff. TMG auf sämtliche sonstige Datenerhebungen, -verarbeitungen und -nutzungen von Telemedien Anwendung finden. Grundsätzlich muss allerdings ein Anbieter-Nutzer-Verhältnis vorliegen.[51] Dies ist für Online-Spiele von besonderer Bedeutung, wenn personenbezogene Daten nur zwischen Nutzern eines Dienstes Verwendung finden und der Betreiber des Online-Spiels insoweit in diesen Prozess nicht eingebunden ist (z. B. bei reinen LAN-Spielen oder bei direkter Verbindung der eingesetzten Spiele-Clients).

Grundsätzlich schützen die datenschutzrechtlichen Regelungen des TMG demnach den Nutzer von Telemedien. Nutzer im Sinne des TMG ist gemäß § 11 Abs. 2 TMG jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen. Bei letzterer Auflistung handelt es sich nicht um eine abschließende Rege-

[49] Jotzo, in: MMR 2009, S. 232 (234); Schaar, CR 2006, S. 619 (620).

[50] Roßnagel, in: NVwZ 2007, S. 743 (744).

[51] Heckmann in: jurisPK-Internetrecht, Kapitel 1.11, Rn. 19.

lung, sondern nur um eine exemplarische Darstellung der wohl häufigsten Nutzungsarten von Telemedien.

§ 11 Abs. 3 TMG schließt die Anwendung der §§ 11-15 TMG für Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, aus, mit Ausnahme des § 15 Abs. 8 (Speicherung von Nutzungsdaten zum Zwecke der Rechtsverfolgung) und § 16 Abs. 4 Nr. 3 TMG (Bußgeld bei Verstoß gegen § 15 Abs. 8 TMG). Hiervon betroffen sind in erster Linie Access- und E-Mail-Provider.[52]

Der positiven Formulierung des § 12 Abs. 1 TMG lässt sich entnehmen, dass die Datenschutzbestimmungen des TMG ausschließlich für diejenigen personenbezogenen Daten Anwendung finden, die bei der Bereitstellung der Telemediendienste anfallen.

Im Ergebnis bleibt für Online-Spiele demnach festzuhalten, dass die Bereitstellung eines Online-Spiels in Form eines Telemediendienstes unter die datenschutzrechtlichen Bestimmungen des TMG fallen, die Übertragungen der personenbezogenen Daten durch Telekommunikationsanbieter (Nachrichten / E-Mail) unter die Regelungen des TKG und die anderen personenbezogenen Daten in der Regel unter die Bestimmungen des BDSG.[53]

5.2 Verhältnis der Datenschutzregelungen zueinander

Entsprechend den vorgehenden Ausführungen finden sich Bestimmungen zum Datenschutz im nicht-öffentlichen Bereich im Recht der Europäischen Union, in allen nationalen Rechtsordnungen der Mitgliedstaaten und in den Rechtsordnungen von Nicht-EU-Staaten. Da die Betreiber der untersuchten Spiele in unterschiedlichen Staaten ihren satzungsmäßigen Sitz haben und in unterschiedlichen Formen und an unterschiedlichen Orten personenbezogene Daten erheben, verarbeiten oder nutzen, ist im Folgenden zu erörtern, in welchen Fällen welche Datenschutzbestimmungen Anwendung finden. Hierbei helfen im Bereich des Rechts der Europäischen Union die Kollisionsvermeidungsnormen der EG-Datenschutzrichtlinie.

Wie bereits in Abschnitt 5.1.1 erörtert, kommen die internationalen Datenschutzbestimmungen als Prüfungsmaßstab für den Datenschutz in Online-Spielen nicht in Betracht, da sie keinen verbindlichen Rechtscharakter aufweisen. Auch die aufgeführten Richtlinien selbst sind nicht unmittelbar anwendbar und können allenfalls für Auslegungsfragen herangezogen werden. Anknüpfungspunkt für die Bestimmung des anwendbaren Rechts ist demnach das Recht der nach internationalen Vorschriften anwendbaren Rechtsordnung. Daher ist regelmäßig nationales Recht anwendbar. Welches nationale Recht anwendbar ist, bestimmt sich nach den Beteiligten an einem Sachverhalt und dem Ort, an dem die Beteiligten ihren Hauptsitz oder ihren gewöhnlichen Aufenthalt oder ihren Standort haben.[54]

---

[52] BT-Drs. 16/3078, S. 15 Gesetzesbegründung zum TMG.

[53] Schleipfer, in: DuD 2004, S. 727 (732); Rost, Welches Gesetz gilt eigentlich?, https://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm/.

[54] Helfrich, in: Hoeren / Sieber (Hrsg.), Handbuch Multimedia-Recht, 2008, Teil 16.1 Rn. 104.

5.2.1 EG-Datenschutzrichtlinie: Territorialitäts- und Niederlassungsprinzip

Erster Anknüpfungspunkt für die Bestimmung der einschlägigen Rechtsordnung ist gemäß Art. 4 Abs. 1 lit. a) der EG-Datenschutzrichtlinie der Sitz einer verantwortlichen Stelle. Dies resultiert daraus, dass innerhalb der Europäischen Union das Recht des Sitzes der Hauptniederlassung gilt[55] und der Hauptsitz eines Unternehmens sich im Verhältnis zu anderen Kriterien meist leicht bestimmen lässt. Sitztheorie bedeutet, dass für das anwendbare Recht auf dem Gebiet der Europäischen Union der satzungsmäßige Sitz eines handelnden Unternehmens maßgeblich ist.

Für den weiteren Gang der Studie bedeutet Art. 4 Abs. 1 lit. a) EG-Datenschutzrichtlinie im Grundsatz, dass jeweils diejenige Rechtsordnung eines Mitgliedstaates Anwendung findet, in welchem sich der satzungsmäßige Sitz eines Daten verwendenden Unternehmens befindet. Von diesem Grundsatz macht Art. 4 Abs. 1 lit. a) EG-Datenschutzrichtlinie jedoch dann eine Ausnahme, wenn ein Unternehmen eine Niederlassung in einem Mitgliedstaat hat und im Rahmen der Tätigkeit dieser Niederlassung personenbezogene Daten verwendet werden. In diesem Fall ist das Recht desjenigen Mitgliedstaates anwendbar, in dessen Hoheitsgebiet sich die Daten verwendende Niederlassung befindet. Insoweit gilt im Datenschutzrecht im Gebiet der Europäischen Union das Niederlassungsprinzip als eine Einschränkung der Sitztheorie.

Daher ist es für das anwendbare Recht unerheblich, wo die Daten erhoben werden oder wo der Betroffene seinen gewöhnlichen Aufenthalt hat. Ausschlaggebend ist, dass die im Inland befindliche Niederlassung die personenbezogenen Daten erhebt, verarbeitet oder nutzt. Für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten, in denen jeweils personenbezogene Daten erhoben, genutzt oder verarbeitet werden, folgt daraus jedoch auch, dass die jeweiligen Niederlassungen das jeweilige nationale Recht berücksichtigen müssen. Im Ergebnis dürfte dies für die Unternehmen wenig Bedeutung haben, da im Rahmen des Binnenmarktes aufgrund der Harmonisierung durch die EG-Datenschutzrichtlinie einheitliche Datenschutzbestimmungen gelten.

Diese Ausführungen gelten aufgrund der Umsetzungsregelung von EU-Rechtsakten im Abkommen über den Europäischen Wirtschaftsraum (EWR) auch für die Staaten Liechtenstein, Island und Norwegen.[56]

Exemplarisch sollen im Folgenden für Deutschland mögliche Fallkonstellationen dargestellt werden.

---

[55] EuGH, Rs. C-208/00 (Überseering BV./.Nordic Construction Company Baumanagement GmbH), Slg. 2002, S. I-9919, Tz. 33.

[56] Anhang XI 5e.01 zur EWR-Rechtssammlung 6. November 2009, http://www.llv.li/pdf-llv-sewr-ewr_register.pdf.

5.2.1.1 Datenschutzrelevante Handlungen eines Unternehmens mit Hauptsitz in Deutschland ohne weitere Niederlassung (Hauptsitz in Deutschland, keine Niederlassung)

Dies ist der einfachste zu regelnde Fall. Hier finden die Bestimmungen des deutschen Datenschutzrechts uneingeschränkte Anwendung, da es sich um einen rein nationalen Sachverhalt ohne grenzüberschreitenden Bezug handelt.

5.2.1.2 Datenschutzrelevante Handlungen einer in Deutschland bestehenden Niederlassung, einer im EU-Ausland ansässigen verantwortlichen Stelle (Hauptsitz im EU-Ausland, Daten verwendende Niederlassung in Deutschland)

Gemäß der Formulierung in der EG-Datenschutzrichtlinie findet in diesen Fällen nach Art. 4 Abs. 1 lit. a) EG-Datenschutzrichtlinie diejenige Rechtordnung Anwendung, in deren Hoheitsgebiet sich die tätige Niederlassung befindet. Im Ergebnis wäre hier deutsches Datenschutzrecht anzuwenden, unabhängig davon, ob die Niederlassung für die Datenverarbeitung oder -nutzung auf Server in anderen Staaten zugreifen muss. Dieses Ergebnis deckt sich auch mit § 1 Abs. 5 Satz 1 letzter Halbsatz BDSG.

Die nationalen deutschen Datenschutzbestimmungen kommen gemäß § 1 Abs. 5 BDSG zur Anwendung, wenn die datenschutzrelevant handelnde Niederlassung eines Unternehmens im Gebiet der Bundesrepublik Deutschland gelegen ist. Demnach findet deutsches Datenschutzrecht, unabhängig von der Datenverarbeitung, im In- oder Ausland dann Anwendung, wenn der Publisher oder Betreiber der Online-Spiele eine Niederlassung in Deutschland hat. Dies gilt nach § 3 Abs. 1 TMG auch für die Daten, die zur Erbringung des Online-Spiels anfallen.

5.2.1.3 Datenschutzrelevante Handlungen einer im EU-Ausland ansässigen verantwortlichen Stelle auf deutschem Territorium ohne tätige Niederlassung in Deutschland (Hauptsitz im EU-Ausland, Daten verwendende Niederlassung im EU-Ausland)

Die deutschen Datenschutzbestimmungen finden gemäß § 1 Abs. 5 S. 1 erster Halbsatz BDSG in diesem Fall keine Anwendung, da das Daten verwendende Unternehmen keine Niederlassung in Deutschland hat. Es findet dasjenige Datenschutzrecht des Mitgliedstaates Anwendung, in dessen Hoheitsgebiet die Niederlassung tätig ist. Dies gilt auch nach § 3 Abs. 1 TMG für Daten, die zur Erbringung des Online-Spiels anfallen.

Im Ergebnis können damit Unternehmen, die ausschließlich in einem Mitgliedstaat der Europäischen Union tätig sind, auf die für sie innerstaatlich geltenden Datenschutzbestimmungen zurückgreifen. Sie müssen für die Erhebung, Nutzung und Verarbeitung personenbezogener Daten im europäischen Ausland keine zusätzlichen ausländischen Datenschutzbestimmungen berücksichtigen. Sinn und Zweck dieser Regelung ist es, kleinere und mittlere Unternehmen, die nur einen Hauptsitz haben, zu unterstützen. Diese Regelung birgt insoweit auch für deutsche Online-Spieler keine Gefahr, als alle Mitgliedstaaten der Europäischen Union aufgrund der EG-Datenschutzrichtlinie ein einheitliches Datenschutzniveau aufweisen müs-

sen. Im Hinblick auf den Schutz der Nutzungs- und Bestandsdaten nach dem TMG sind § 3 Abs. 1 und 2 TMG zu berücksichtigen. Danach ist das Recht des Ortes der Niederlassung maßgeblich.

5.2.1.4 Zwischenergebnis

Entsprechend den vorgehenden Ausführungen gilt für den Anwendungsbereich der EG-Datenschutzrichtlinie, dass deutsches Datenschutzrecht grundsätzlich dann Anwendung findet, wenn sich eine Niederlassung eines Unternehmens mit Hauptsitz auf dem Gebiet der Europäischen Union im Hoheitsgebiet der Bundesrepublik Deutschland befindet und personenbezogene Daten erhebt, nutzt oder verwendet. Dies gilt auch, wenn personenbezogene Daten ausschließlich von einem Unternehmen mit Hauptsitz in Deutschland und ohne weitere Niederlassung erhoben werden. BDSG und TMG finden entsprechend den Vorgaben der EG-Datenschutzrichtlinie keine Anwendung, wenn die personenbezogenen Daten von einer Niederlassung in einem anderen EU-Mitgliedstaat verwendet werden, unabhängig vom Hauptsitz des Unternehmens und dem Ort der Erhebung der personenbezogenen Daten.

5.2.2 Drittstaatenregelungen

Im Folgenden bleibt zu klären, welches Datenschutzrecht zur Anwendung kommt, wenn der Spieler in Deutschland seinen gewöhnlichen Aufenthalt hat, der Betreiber des Online-Spiels seinen Hauptsitz in einem Drittstaat außerhalb der EU hat und innerhalb der Europäischen Union keine weitere tätige Niederlassung besitzt. Dies ist im Rahmen von Online-Spielen eine wichtige Konstellation, da viele Betreiber von Online-Spielen ihren Hauptsitz in einem Staat außerhalb der Europäischen Union haben.

Maßgeblich ist in diesem Zusammenhang die Regelung des § 1 Abs. 5 Satz 2 BDSG. Danach ist das BDSG anwendbar, wenn eine verantwortliche Stelle personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt, die keine Niederlassung in einem anderen Mitgliedstaat der Europäischen Union besitzt. Anders als innerhalb der Europäischen Union gilt in diesen Fällen daher das Territorialitätsprinzip. Insoweit ist in diesen Fällen, anders als im Anwendungsbereich der EG-Datenschutzrichtlinie, der Ort der Erhebung, Nutzung oder Verarbeitung personenbezogener Daten maßgeblich. Dies gilt gemäß § 1 Abs. 5 Satz 2 BDSG jedoch nicht für den reinen „Transitverkehr“ durch Deutschland.

Ist das BDSG anwendbar, wenn personenbezogene Daten in Deutschland erhoben, verarbeitet oder genutzt werden, so stellt sich die Frage, wann eine in einem Drittstaat angesiedelte verantwortliche Stelle personenbezogene Daten in Deutschland erhebt, nutzt oder verarbeitet. Personenbezogene Daten werden gemäß § 3 Abs. 3 BDSG erhoben, wenn sie vom Betroffenen beschafft werden. Dabei ist es ist erforderlich, dass die verantwortliche Stelle

das Beschaffen aktiv betreibt.[57] Eine zufällige Gewinnung von Daten fällt nicht unter den Begriff „Erheben".[58]

Insoweit ist zu ermitteln, welcher Ort ausschlaggebend für die Erhebung von personenbezogenen Daten ist. In Betracht kommt einerseits der Standort des Servers, da die personenbezogenen Daten am Server endgültig anfallen, andererseits könnte auch der Standort des Spieler-PCs maßgeblich sein, da dieser seine personenbezogenen Daten an diesem Standort zur Verfügung stellt. Eine dritte Möglichkeit besteht darin, unabhängig von den Standorten der Hardware und der Nutzung des Spiels durch den Spieler an den Erhebungswillen der verantwortlichen Stelle anzuknüpfen. Eine Aussage dazu trifft das BDSG nicht. Da gemäß Art. 10 EG die mitgliedstaatlichen Stellen auch zu einer richtlinienkonformen Auslegung des nationalen Rechts verpflichtet sind, ist ergänzend Art. 4 Abs. 1 lit. c) der EG-Datenschutzrichtlinie heranzuziehen. Ausgehend von Prinzip der aktiven Erhebung ist auch im Falle des maßgeblichen Orts die Aktivität des Publishers/Betreibers zu berücksichtigen.

Geht man von der ersten Möglichkeit aus, so hätte dies zur Folge, dass der Serverbetreiber mit Aufstellen des Servers Rechtssicherheit hinsichtlich des anwendbaren Datenschutzrechts hätte.[59] Für die Online-Spieler ist dies jedoch insoweit nachteilig, als sie teilweise keinen Einfluss darauf haben, auf welchem Server ihre personenbezogenen Daten erhoben, verarbeitet und genutzt werden. Der Spieler kann dies auch nicht immer nachvollziehen, weder vor noch während oder nach der Erhebung, Verarbeitung oder Nutzung. Spiele-Betreiber bzw. Serverbetreiber könnten sich allein mit der Behauptung, der betroffene Server befände sich in einem Drittstaat, den Datenschutzbestimmungen der EG-Datenschutzrichtlinie bzw. den nationalen Datenschutzbestimmungen entziehen.

Dieser Argumentation könnte man entgegen treten, wenn der Standort des PCs des Spielers maßgeblich wäre.[60] Dies könnte jedoch dazu führen, dass ein Spiele-Betreiber in einem Drittstaat, der einen Server in diesem Drittstaat nutzt und sein Angebot sprachlich an die Spieler in diesem Drittstaat richtet, in dem Moment, in dem ein deutscher Spieler das Spielangebot nutzt, deutsches Datenschutzrecht zu berücksichtigen hätte. Dies würde zwar zu einem voll umfänglichen Schutz der deutschen Spieler führen und dem Grundgedanken des Schutzes der Betroffenen entsprechen, den Spiele-Betreiber jedoch vor nahezu unlösbare Probleme stellen. Der Betreiber selbst hat keinen direkten Einfluss auf die teilnehmenden Online-Spieler. Die Teilnahme eines Spielers mit Aufenthalt in Deutschland würde in diesem Fall den Spiele-Betreiber verpflichten, die deutschen Datenschutzbestimmungen anzuwenden. Die Teilnahme eines Spielers mit Aufenthalt in Japan würde eine Anwendbarkeit des japanischen Datenschutzrechts verlangen. Dies führt zu unterschiedlich anwendbaren Be-

---

57 Weichert, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 1 Rn. 19.

58 Jotzo, in: MMR 2009, S. 232 (235).

59 Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1 Rn. 223.

60 Scheja, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, S. 90.

stimmungen für einen Betreiber. Möchte er nicht Teilnehmer aus bestimmten Staaten von vornherein ausschließen, so muss er sämtliche Datenschutzbestimmungen einhalten. Dies wird faktisch wohl nicht möglich sein, insbesondere, da sich derartige Regelungen in Ermangelung eines Welt-Datenschutzrechts sogar widersprechen können.

Da sowohl der Ansatz des Standorts des Servers als auch derjenige des Standorts des Spieler-PCs Schwächen aufweisen, wird als dritte Möglichkeit vertreten, dass allein maßgeblich das Angebot des Spiele-Betreibers sei. Richtet sich die Webseite mit ihrem Angebot an deutsche Spieler, ist sie in deutscher Sprache verfasst und handelt es sich bei der Top-level-domain um die deutsche Domain „de“, so soll deutsches Datenschutzrecht anwendbar sein. Der Publisher / Betreiber, der in diesem Fall personenbezogene Daten erhebt, hat einen konkreten Erhebungswillen bezogen auf personenbezogene Daten in Deutschland. Dieser Ansatz wird gestützt durch Erwägungsgrund 20 der EG-Datenschutzrichtlinie.[61] Danach soll eine Niederlassung eines Verantwortlichen für die Datenverarbeitung in einem Drittstaat nicht zu einem geringeren Schutz der Spieler in der Europäischen Union führen.

Vom Bundesgerichtshof wurde im Hinblick auf das Wettbewerbsrecht der Grundsatz des Marktortprinzips aufgestellt.[62] Danach ist in Fällen, in denen vom Ausland zielgerichtet auf Märkte im Inland eingewirkt wird, das jeweilige nationale Recht anwendbar. Dementsprechend hat der BGH bei Wettbewerbsverletzungen im Internet die Wettbewerbsregelungen des Staates angewandt, in welchem sich der Webauftritt bestimmungsgemäß auswirken soll.[63] Das VG Düsseldorf geht davon aus, dass bei Glücksspielen, welche grenzüberschreitend angeboten werden, nach völkerrechtlichen Grundsätzen zur Begründung der Regelungskompetenz eines Staates ein Anknüpfungspunkt im Inland ausreicht.[64]

Dieser marktorientierte Ansatz berücksichtigt nicht nur das Schutzinteresse des Spielers, sondern auch das Interesse des Betreibers vorhersehen zu können, welche Datenschutzbestimmungen für sein Angebot maßgeblich sind. Zusätzlich kann ein Vergleich mit dem europäischen Verbraucherschutz herangezogen werden. Im Datenschutz und im Verbraucherschutz besteht eine vergleichbare Interessenlage. In beiden Bereichen wurden auf Ebene der Europäischen Union einheitliche Schutzstandards entwickelt.

Anerkannt ist inzwischen, dass beim Ausfüllen eines Online-Formulars zwischen der verantwortlichen Stelle für die Übermittlung der Daten und der die Daten abfragenden Stelle zu unterscheiden ist. Entscheidet der Betroffene selbst über die Eingabe und Weitergabe seiner Daten an eine Webseite, so ist er zu diesem Zeitpunkt verantwortliche Stelle. Dammann geht davon aus, dass es sich bei einem Angebot, mittels einer Webseite Daten zu senden, um

---

61 Erwägungsgrund 20 Ri 95/46/EG.

62 BGH, Urteil vom 30. März 2006, Az.: I ZR 24/03, BGHZ 167, S. 91.

63 BGH, Urteil vom 30. März 2006, Az.: I ZR 24/03, BGHZ 167, S. 91.

64 VG Düsseldorf, Beschluss vom 24. Juni 2009, Az.: 27 L 1131/08, juris, Rn. 95.

eine Art „invitatio ad offerendum“ handelt.[65] Der Spieler selbst hat in diesem Moment die Entscheidungsgewalt darüber, ob er die Daten senden möchte. Insoweit werden noch keine Daten erhoben. Anders hingegen ist dies, wenn der Betreiber einer Webseite, ein Programm auf dem PC des Spielers installiert, welches dem Betreiber die Möglichkeit gibt, Informationen unabhängig vom Spieler abzurufen, dieser also im Zweifel in dem Abrufmoment nicht nachvollziehen kann, dass personenbezogene Daten und welche Daten abgerufen werden (z. B. Cookies).

Im Bereich der Nutzung und Verarbeitung der Daten genügt es daher nach dieser Theorie für die Anwendbarkeit der deutschen Datenschutzbestimmungen, dass diese Daten in Deutschland belegen sind. Dies bedeutet, dass die Daten auf einem Server in Deutschland abgespeichert sind und von dort auch im Drittland abgerufen werden können.[66]

Im Ergebnis ist deutsches Datenschutzrecht nach der hier vertretenen Auffassung anwendbar, wenn sich Betreiber mit ihren Spielangeboten an Spieler auch in Deutschland richten. Dies ist insbesondere dann anzunehmen, wenn die Angebote in deutscher Sprache gehalten sind bzw. eine entsprechende Sprachauswahl möglich ist und das Angebot unter einer deutschen (Top-Level) Domain bereitgestellt wird. Betreibern, die sich insoweit konkret an den deutschen Markt richten, ist es zuzumuten, die deutschen Datenschutzbestimmungen zu berücksichtigen.

5.2.3 Besonderheiten für Telemedien

Besonderheiten gelten im Zusammenhang mit dem räumlichen Anwendungsbereich der Datenschutzbestimmungen für Telemedien. Diese betreffen insbesondere Bestands- und Nutzungsdaten, die bei der Bereitstellung von Online-Spielen verarbeitet werden. § 3 des TMG regelt insoweit eine eigene Zuständigkeit, soweit das TMG sachlich anwendbar ist. Auch das TMG geht in entsprechender Umsetzung der Richtlinie 2000/31/EG (EG-Telemedienrichtlinie) davon aus, dass maßgeblich der Niederlassungsort des Diensteanbieters ist.[67] Es ist demnach unabhängig davon, wo die Telemediendienste angeboten werden. Der Diensteanbieter unterliegt dem Recht des Mitgliedstaates, in dem er seine Niederlassung hat.

Für in Deutschland (auch) niedergelassene Telemediendiensteanbieter gilt daher grundsätzlich das deutsche Recht, auch wenn die jeweiligen Dienste in einem anderen Mitgliedstaat der Europäischen Union oder in Liechtenstein, Island und Norwegen angeboten oder erbracht werden. In einem anderen Mitgliedstaat der EU oder des EWR niedergelassene Telemedienanbieter unterliegen den rechtlichen Bestimmungen des jeweiligen Mitgliedstaates. Eine derartige Regelung benachteiligt auch deutsche Verbraucher nicht, da das Schutzni-

[65] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1 Rn. 223.

[66] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1 Rn. 221.

[67] Heckmann, in: jurisPK-Internetrecht, Kapitel 1.3, Rn. 4.

veau im Geltungsbereich des EU-Vertrages und des EWR-Abkommens aufgrund der Harmonisierung der jeweiligen Vorschriften (großteils) einheitlich ist.

Unabhängig davon ist in § 3 Abs. 3 Nr. 4 TMG jedoch geregelt, dass diese Bestimmungen und die Einschränkungen des Absatzes 2 nicht für die nationalen Datenschutzbestimmungen gelten. Hier ist vielmehr die Regelung des § 1 Abs. 5 BDSG zu berücksichtigen. Im Ergebnis ist daher § 1 Abs. 5 BDSG als Kollisionsregelung anzuwenden und führt dazu, dass auch die §§ 11 ff. TMG international Anwendung finden.

5.3 Inhaltlich relevante Grundsätze des Datenschutzrechts mit Bezug zu Online-Spielen

Den aufgeführten nationalen und internationalen Datenschutzbestimmungen lassen sich Grundsätze entnehmen, welche für Online-Spiele und deren datenschutzkonforme Entwicklung und Nutzung als Leitlinien herangezogen werden können und müssen. Erforderlich für die Anwendbarkeit der Datenschutzgesetze ist, dass die Daten einen Personenbezug aufweisen. Für die Bestimmung der einschlägigen Normen ist es notwendig, die verantwortliche Stelle für die personenbezogenen Daten zu kennen.

5.3.1 Personenbezogene Daten

Ausschlaggebend für die erforderliche Berücksichtigung der Datenschutzgrundsätze ist ein Personenbezug der in Frage stehenden Daten. Ein Personenbezug von Daten ist regelmäßig dann anzunehmen, wenn es sich um Informationen über eine bestimmte oder bestimmbare natürliche Person handelt (Art. 2 lit. a) EG-Datenschutzrichtlinie, § 3 Abs. 1 BDSG). Insoweit werden alle Angaben erfasst, die einer Person zugeordnet werden können. Für die Anwendbarkeit der datenschutzrechtlichen Bestimmungen des TMG ist grundsätzlich von einem weiten Begriff des personenbezogenen Datums auszugehen.[68] Für Online-Spiele bedeutet dies, dass alle Daten, die einen Rückschluss auf einen bestimmten Spieler zulassen, unter den Begriff des personenbezogenen Datums fallen. Dies bedeutet auch, dass alle in den einzelnen Phasen des Online-Spielens – vom Kauf des Spiels über die Installation, die Bezahlung und das Spielverhalten bis zur Kommunikation im Spiel – anfallenden Daten einen Personenbezug aufweisen können.

Für den Betreiber kann z. B. von Belang sein, welche Geschwindigkeit die Internetverbindung eines Spielers hat. Dies kann Aufschluss über die technischen Möglichkeiten der Spielverbindung geben und für die Bewerbung einzelner Spiele interessant sein, da bestimmte Spiele bestimmte technische Voraussetzungen erfordern. In der Zusammenschau mit weiteren identifizierenden Daten, können dann auch diese Informationen einen Personenbezug haben und Aussagen über die technische Ausstattung des Spielers treffen.

[68] Heckmann, in: jurisPK-Internetrecht, Kapitel 1.12, Rn. 10.

5.3.2 Verantwortliche Stelle und Telemediendiensteanbieter

Die Einhaltung der Datenschutzgrundsätze müssen die für die Datenverarbeitung Verantwortlichen gewährleisten. Verantwortlich in diesem Sinne sind nach § 3 Abs. 7 BDSG die natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Im Gegensatz dazu ist ein Auftragsdatenverarbeiter – eine Person oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verwendet – nicht selbst gegenüber dem Spieler verantwortlich für die Einhaltung der Datenschutzgrundsätze in Bezug auf die entsprechenden Daten, siehe § 3 Abs. 7 und § 11 Abs. 1 Satz 1 BDSG. Bei der Nutzung von Telemedien ist grundsätzlich der Diensteanbieter bzw. Betreiber verpflichtet, die Einhaltung der Regelungen der §§ 11 ff. TMG zu gewährleisten.

5.3.3 Datenschutzrechtliche Grundsätze

Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, so sind die Verantwortlichen bzw. Betreiber verpflichtet, die sich für natürliche Personen aus den Datenschutzbestimmungen ergebenden Rechte zu gewährleisten. Den Bestimmungen der EG-Datenschutzrichtlinie lassen sich verschiedene Grundsätze für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten entnehmen. Diese Grundsätze erfahren durch die weiteren Bestimmungen noch darzustellende Einschränkungen. Generell muss die Datenverwendung den Grundsätzen der Rechtmäßigkeit Art. 6 Abs. 1 lit. a) EG-Datenschutzrichtlinie, Erforderlichkeit Art. 6 Abs. 1 lit. c) EG-Datenschutzrichtlinie, der Datenvermeidung und Datensparsamkeit Art. 6 Abs. 1 lit. c) EG-Datenschutzrichtlinie, Zweckbindung Art. 6 Abs. 1 lit. b) EG-Datenschutzrichtlinie, Transparenz Art. 10 EG-Datenschutzrichtlinie sowie Datensicherheit Art. 17 EG-Datenschutzrichtlinie entsprechen.

5.3.3.1 Grundsatz der Rechtmäßigkeit – Erlaubnisvorbehalt

Im Grundsatz dürfen personenbezogene Daten unabhängig von dem Medium erhoben, verarbeitet und genutzt werden, wenn eine Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt (Art. 7 EG-Datenschutzrichtlinie, § 4 Abs. 1 BDSG, § 12 Abs. 1 letzte Alternative TMG). Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten steht damit unter einem Gesetzesvorbehalt. Juristisch wird von einem Verbot mit Erlaubnisvorbehalt gesprochen.[69] Diese Regelung schützt das Grundrecht auf informationelle Selbstbestimmung.[70] Jede natürliche Person soll in die Lage versetzt werden, selbst darüber zu bestimmen, welche personenbezogenen Daten erhoben, genutzt oder verarbeitet werden dürfen und wo diese Daten verwendet werden. Im Ergebnis ist demnach eine Verwendung

[69] Tinnefeld / Ehmann / Gerling, Einführung in das Datenschutzrecht, 4. Auflage 2005, S. 316.

[70] BVerfGE 65, S. 1 (46).

personenbezogener Daten ohne Einwilligung des Betroffenen oder Rechtsgrundlage unzulässig.

5.3.3.2 Grundsatz der freiwilligen informierten Einwilligung

Grundsätzlich wird im europäischen Datenschutzrecht von einem Einwilligungserfordernis ausgegangen, Art. 2 lit. h) EG-Datenschutzrichtlinie. Dieses ist in das deutsche Recht mit § 4a BDSG und § 12 TMG umgesetzt worden. Die Spiele-Betreiber sind entsprechend diesen Vorschriften verpflichtet zu prüfen, ob die Spieler eine wirksame Einwilligung für die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten erteilt haben. Eine Einwilligung ist eine Willenserklärung des Betroffenen dahingehend, dass seine personenbezogenen Daten erhoben, verarbeitet und genutzt werden dürfen. Diese muss freiwillig für den konkreten, ihm bekannten Sachverhalt erteilt worden sein.

Eine Einwilligung soll in der Regel schriftlich erteilt werden. Soweit Daten im Rahmen einer elektronischen Kommunikation erhoben, verarbeitet oder genutzt werden, ist eine Einwilligung auch in dieser Form möglich. § 13 Abs. 2 TMG setzt insoweit Erwägungsgrund 17 der EG-Datenschutzrichtlinie um und bestätigt, dass auch Online-Spiele-Betreiber eine elektronische Einwilligung zur Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten erhalten können.[71] Die Form der Einwilligung muss allerdings sicherstellen, dass der Spieler seine Einwilligung bewusst und eindeutig erteilt, die Einwilligung protokolliert wird, der Spieler den Inhalt der Einwilligung jederzeit abrufen und mit Wirkung für die Zukunft widerrufen kann.

5.3.3.3 Grundsatz der Zweckbindung

Weiterhin dürfen personenbezogene Daten nur für den Zweck verwendet werden, für den sie erhoben wurden (Art. 6 Abs. 1 lit. c) EG-Datenschutzrichtlinie, § 28, 29 BDSG, § 12 Abs. 2 TMG). Dieser Grundsatz sichert für den Nutzer die Transparenz der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten. Eine über den Erhebungszweck hinausgehende Nutzung oder Verarbeitung der personenbezogenen Daten des Nutzers ist ohne seine Einwilligung oder eine weitere Erlaubnisnorm nicht zulässig.

Viele „Hauptzwecke“, zu denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind in den §§ 28 und 29 BDSG aufgeführt. Dabei handelt es sich zwar lediglich um Beispiele, die nicht abschließend aufgezählt werden; es hat sich aber gezeigt, dass sie einen Großteil der typischen Datenerhebungen abdecken. So können personenbezogene Daten von Unternehmen für eigene (§ 28 BDSG) oder für fremde (§ 29 BDSG) Geschäftszwecke erhoben werden. Anerkannte Zwecke für die eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erforderlich sein kann, sind unter anderem Vertragserfüllung,

[71] Heckmann, in: jurisPK-Internetrecht, Kapitel 1.12, Rn. 53.

Gefahrenabwehr, Werbung, Markt- und Meinungsforschung und auf anderen berechtigten Interessen beruhende Zwecke, die jedoch ausreichend spezifiziert sein müssen.

Eine Zweckänderung während der Nutzung ist grundsätzlich möglich. Für diese bedarf es allerdings einer weiteren Erlaubnisnorm. Der Grundsatz der Rechtmäßigkeit muss insoweit erneut erfüllt werden; für die Zweckänderung ist daher erneut eine Einwilligung des Betroffenen oder eine Rechtsgrundlage erforderlich. Rechtsnormen, welche eine Zweckänderung der Nutzung der personenbezogenen Daten rechtfertigen, lassen sich ebenfalls im BDSG (§ 28 Abs. 3 BDSG) und im TMG (§ 14 Abs. 2, § 15 Abs. 3, 4, 8 TMG) finden.

5.3.3.4 Grundsatz der Erforderlichkeit

Im Zusammenhang mit der Zweckbindung der Datenverarbeitung steht der Grundsatz der Erforderlichkeit. Der Grundsatz der Erforderlichkeit findet seinen Niederschlag in Art. 6 und 7 der EG-Datenschutzrichtlinie. Dies bedeutet, dass nur diejenigen Daten erhoben, verarbeitet und genutzt werden dürfen, die für den jeweiligen Zweck erforderlich sind. Eine über den Zweck hinausgehende Erhebung personenbezogener Daten ist in der Regel nicht zulässig. Im Ergebnis bedeutet dies, dass für jeden Vorgang erneut überprüft werden muss, welche Daten für diesen Vorgang überhaupt notwendig sind und ob eventuell der Personenbezug nicht erforderlich ist und die Daten dementsprechend gar nicht erst erhoben oder möglichst bald anonymisiert, pseudonymisiert oder gelöscht werden können.

Im Rahmen von Online-Spiele bedeutet dies schon für den Hersteller, in jeder Phase die Erforderlichkeit von Daten und deren etwaigem Personenbezug zu prüfen und die technischen Vorkehrungen zu schaffen, dass Daten nur in dem erforderlichen Umfang erhoben, verarbeitet und genutzt werden. Eine immer mögliche Verfügbarkeit aller erhobenen Daten ist in den seltensten Fällen erforderlich. Daraus folgt insbesondere, dass personenbezogene Daten, die für Vorgänge nicht (mehr) erforderlich sind, zu löschen sind und nicht auf Vorrat gehalten werden dürfen.

5.3.3.5 Grundsatz der Transparenz

Für den Betroffenen, in Online-Spielen also für den Spieler, muss die Erhebung, Verarbeitung und Übermittlung seiner personenbezogenen Daten transparent sein. Dies bedeutet, dass es jedem Spieler von Online-Spielen möglich sein muss zu wissen, welche personenbezogenen Daten über ihn an welcher Stelle verfügbar sind. Die datenschutzrechtlichen Bestimmungen des BDSG, TMG und TKG werden diesem Grundsatz insoweit gerecht, als sie Rechte für den Betroffenen und Pflichten für die verantwortliche Stelle, den Telemedien- bzw. Telekommunikationsdienstleister enthalten. So sind in allen Gesetzen Auskunfts-, Löschungs- und Berichtigungsansprüche zu finden, die die Rechte der Betroffenen sichern sollen. Demselben Zwecken dienen bestimmte Informationspflichten der verantwortlichen Stellen, Telemedien- und Telekommunikationsdienstleister.

Für Online-Spiele bedeutet dies, dass der Spieler vor der Erhebung der Daten darüber zu

informieren ist, welche Daten erhoben werden, wann sie erhoben werden und an wen welche Daten übermittelt werden bzw. wem welche Daten zugänglich sind. Werden die personenbezogenen Daten nicht direkt beim Spieler erhoben, so ist dieser nachträglich darüber zu benachrichtigen, welche Daten zu welchem Zweck erhoben, verarbeitet und genutzt werden.

5.3.3.6 Grundsatz der Datensicherheit

Neben diesen materiellen Grundsätzen sind technisch-organisatorische Grundsätze (§ 9 BDSG, § 13 Abs. 4 TMG) bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten von der verantwortlichen Stelle und den Dienstleistern / Auftragnehmern zu beachten. Personenbezogene Daten dürfen nur sicher verarbeitet werden. Bei den technischen Maßnahmen zur Datensicherheit handelt es sich um Sicherheitsmaßnahmen durch technische Konfigurationen.[72] Für Online-Spiele erforderlich sind in diesem Zusammenhang vor allem Maßnahmen zur Zugriffssicherung. Organisatorische Maßnahmen sind solche Maßnahmen, die die Zuständigkeit und Verantwortung für den Schutz der personenbezogenen Daten sichern.

5.3.3.7 Grundsatz der Kontrolle

Abschließend ist die Einhaltung der aufgeführten Datenschutzgrundsätze durch eine geeignete unabhängige Kontrolle der verantwortlichen Stellen und Dienstleister / Auftragnehmer sicherzustellen (Art. 29 EG-Datenschutzrichtlinie). Dies bedeutet, dass die relevanten Stellen in der Regel einen betrieblichen Datenschutzbeauftragten ernennen müssen (§ 4f BDSG). Betreiber von Online-Spielen in Deutschland / Europa müssen sich ebenfalls darüber bewusst sein, dass sie einer Kontrolle durch die jeweils zuständigen Datenschutzbehörden unterliegen. Diese haben neben den Prüfungsrechten auch einen Beratungsauftrag: Daten verarbeitende Stellen können sich an die Aufsichtsbehörden wenden und Beratungen in Anspruch nehmen § 38 Abs. 1 Satz 2 BDSG.

5.4 Grundsatz der Subsidiarität

Soweit auf einen Sachverhalt verschiedene Rechtsnormen Anwendung finden können, ist zu bestimmen, welche der möglichen Rechtsnormen einschlägig ist. Kommt es zu einer Kollision zwischen BDSG und TKG oder TMG, so ist § 1 Abs. 3 BDSG zu berücksichtigen. Diese Norm legt den Grundsatz der Subsidiarität für das BDSG fest. Soweit andere Vorschriften auf den Umgang mit personenbezogenen Daten anwendbar sind, tritt das BDSG hinter diesen Vorschriften zurück.[73] Sollten die entsprechenden Normen Lücken aufweisen, kommt das BDSG ergänzend zur Anwendung.

---

[72] Bizer, in: DuD 2007, S. 350 (355).

[73] Walz, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1 Rn. 269.

Gemäß § 12 Abs. 1 TMG gelten die Datenschutzbestimmungen des 4. Abschnitts des TMG ausschließlich für die Bereitstellung von Telemedien. Andere Rechtsgrundlagen, die eventuell anwendbare Erlaubnisnormen für die Erhebung, Nutzung und Verarbeitung personenbezogener Daten im Bereich der Telemedien enthalten, sind grundsätzlich nur dann anwendbar, wenn sie sich ausdrücklich auf Telemedien beziehen. Insoweit ist dem § 12 Abs. 2 TMG zu entnehmen, dass das BDSG auf die personenbezogenen Daten, die zur Bereitstellung von Telemedien erforderlich sind, nicht anwendbar ist.

Das TMG gilt in diesem Zusammenhang nach § 14 und § 15 TMG ausschließlich für Bestands- und Nutzungsdaten, das BDSG für Inhaltsdaten. Bestandsdaten im Sinne des § 14 TMG sind personenbezogene Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung des Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Insoweit sind vom TMG sämtliche personenbezogenen Daten erfasst, die für den Telemediendienstvertrag erforderlich sind, nicht jedoch solche personenbezogenen Daten, die aufgrund der Nutzung eines Telemediendienstes erhoben, verarbeitet oder genutzt werden. Exemplarisch für Telemediendienstverträge sind die Verträge für die Einrichtung eines Accounts auf einem Spielsystem, Verträge über den Download von Software für Online-Spiele und Verträge über die Teilnahme an Online-Spielen.[74] Da die Entgeltlichkeit kein Tatbestandsmerkmal des § 14 TMG ist, sind auch kostenlose Bereitstellungen von Online-Spielen und die entsprechenden Log-In-Dateien vom Anwendungsbereich des § 14 TMG umfasst. Typische Bestandsdaten sind der Name des Nutzers, die Adresse, die Telefonnummer, die Bankverbindung, der Benutzername und das Passwort.

Im Unterschied zu den Bestandsdaten sind Inhaltsdaten solche, die keinen Bezug zur Bereitstellung der Telemediendienste aufweisen. Die inhaltlichen Angaben zur Ausgestaltung der Telemedien sind unabhängig von der Bereitstellung selbst und daher auch vom BDSG erfasst. § 15 TMG schützt die Nutzungsdaten. Nutzungsdaten sind grundsätzlich Daten, die für die Möglichkeit der Inanspruchnahme von Telemedien und zu deren Abrechnung erforderlich sind.[75] Typische Nutzungsdaten im Rahmen eines Online-Spielbetriebs sind demnach alle Merkmale, die zur Identifikation des Spielers erforderlich sind und Angaben über den Beginn, das Ende und den Umfang des Spiels enthalten, siehe § 15 Abs. 1 Nr. 1 und 2 TMG. Derartige Daten können IP-Adressen des Spielers oder auch Daten über das Verhalten des Spielers während des Spiels sein.

Das TKG ist nach der Definition seines Anwendungsbereichs zu berücksichtigen, wenn ein Telekommunikationsdienst angeboten wird. Telekommunikationsdienste sind in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen (§ 3 Nr. 24 TKG). Hierbei handelt es sich um die technische Seite der Kommuni-

[74] Heckmann, in: jurisPK-Internetrecht, Kapitel 1.14, Rn. 5.

[75] Heckmann, in: jurisPK-Internetrecht, Kapitel 1.15, Rn. 2.

kation. Typische Telekommunikationsdienste sind Nachrichtendienste wie E-Mail, Telefonie und Mobilfunk, aber auch die Bereitstellung der Nutzung des Internets. Bei Online-Spielen kann insbesondere der Austausch von persönlichen Nachrichten unter das TKG fallen.

5.5 Zwischenergebnis

Die deutschen Datenschutzbestimmungen finden grundsätzlich Anwendung auf Online-Spiele. Alle Unternehmen, die in Deutschland datenschutzrelevante Handlungen vornehmen und eine Niederlassung oder einen Hauptsitz in Deutschland haben, müssen die deutschen Datenschutzbestimmungen berücksichtigen. Ergänzend finden diese Regelungen Anwendung, wenn ein Unternehmen, seinen Hauptsitz oder eine Niederlassung nicht im Geltungsbereich der EU oder des EWR hat, aber in Deutschland datenschutzrelevante Handlungen vornimmt.

Hinsichtlich der Anwendbarkeit der unterschiedlichen Datenschutzbestimmungen im BDSG, TMG und TKG ist von der verantwortlichen Stelle zu beachten, dass die Bereitstellung eines Online-Spiels in Form eines Telemediendienstes unter die datenschutzrechtlichen Bestimmungen des TMG fallen, die Verarbeitung personenbezogener Daten durch Telekommunikationsanbieter unter die Regelungen des TKG und die meisten anderen personenbezogenen Daten unter die Bestimmungen des BDSG. Für den Bereich der Bereitstellung des Online-Spiels sind die Datenschutzbestimmungen des §§ 11 ff. TMG vorrangig vor denjenigen des BDSG zu berücksichtigen. Für die technische Abwicklung von Telekommunikation kommt das TKG (§§ 91 ff.) zur Anwendung. Für Inhaltsdaten ist auf das BDSG zurückzugreifen.

Alle drei Gesetze enthalten Datenschutzbestimmungen. Für alle Datenschutzbestimmungen gelten die aufgeführten Grundsätze mit den gesetzlich vorgesehenen Einschränkungen. Die aufgeführten Grundsätze bilden die Grundlage für den Leitfaden zu den einzelnen Funktionalitäten[76].

[76] Siehe dazu Kapitel 9.

6 Relevante Normen für Online-Spiele

Im Folgenden werden die für Online-Spiele relevanten Datenschutznormen aufgeführt. Ausgehend von den Erlaubnisnormen für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten und den Normen zur Zweckänderung werden die Erlaubnisnormen zur Übermittlung personenbezogener Daten in Drittstaaten aufgeführt und die jeweiligen Normen zu den Rechten der Online-Spieler dargestellt.

6.1 Erlaubnisnormen für eine Erhebung, Nutzung oder Verarbeitung personenbezogener Daten

Eine Erhebung, Nutzung oder Verarbeitung personenbezogener Daten ist entsprechend dem oben Gesagten nur zulässig, wenn der Betroffene, d. h. der Spieler, in die Erhebung, Nutzung oder Verarbeitung seiner personenbezogenen Daten eingewilligt hat oder eine Rechtsvorschrift die Datenverwendung erlaubt oder in anderer Form vorsieht. Die Rechtsgrundlage kann entweder dem BDSG oder einer anderen Rechtsvorschrift entnommen werden. Die EG-Datenschutzrichtlinie sieht in Art. 7 verschiedene Erlaubnistatbestände vor. Diese sind in das BDSG, das TMG, das TKG und die jeweiligen Datenschutzgesetze der Mitgliedstaaten der Europäischen Union und des EWR aufgenommen worden.

6.1.1 Verwendung personenbezogener Daten zum Zwecke der Vertragserfüllung

Der wohl wichtigste Erlaubnistatbestand für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist die Vertragserfüllung bzw. die Erfüllung eines vorvertraglichen Verhältnisses (Art. 7 lit. b) EG-Datenschutzrichtlinie, § 28 Abs. 1 Satz 1 Nr. 1 BDSG, § 14 Abs. 1, § 15 TMG). Entsprechend diesen Vorschriften dürfen Betreiber von Online-Spielen personenbezogene Daten erheben, verarbeiten und nutzen, wenn die Daten für die Erfüllung des Spielvertrages oder die Durchführung vorvertraglicher Maßnahmen, die auf Antrag des Spielers erfolgen, erforderlich sind.

6.1.2 Verwendung personenbezogener Daten zum Zwecke der Werbung

Soweit personenbezogene Daten für Werbezwecke erhoben, genutzt und verarbeitet werden, sind § 28 Abs. 3 BDSG, § 12 Abs. 2 und § 15 Abs. 3 TMG zu beachten. Gemäß § 28 Abs. 3 Satz 2 Nr. 1 BDSG können personenbezogene Daten zum Zwecke der Werbung für eigene Geschäftszwecke erhoben, verarbeitet und genutzt werden, wenn der Betroffene eingewilligt hat oder die Daten listenmäßig oder sonst über Angehörige einer Personengruppe

zusammengefasst sind.[77] Zu beachten ist aber auch dabei das schutzwürdige Interesse des Betroffenen oder dessen Widerspruch.

Soweit es sich bei Online-Spielen um Telemedien handelt, richtet sich die Einwilligung in die Datenverarbeitung für die Werbung nach § 12 Abs. 2 TMG. Ergänzend gilt gemäß § 15 Abs. 3 TMG, dass der Telemediendiensteanbieter (her: Betreiber des Online-Spiels) Nutzungsdaten für Zwecke der Werbung verwenden und Nutzungsprofile erstellen darf. Diese Profile dürfen jedoch nur unter Nutzung von Pseudonymen und nur mit den regulär angefallenen Nutzungsdaten erstellt werden; darüber hinausgehende personenbezogene Daten dürfen für Werbezwecke ohne Einwilligung nicht verwendet werden. Die Spieler sind müssen diesem auch widersprechen können, worauf sie im Rahmen der Datenschutzerklärung hingewiesen werden müssen.

6.1.3 Verwendung personenbezogener Daten zum Zwecke der Markt- und Meinungsforschung

Für Markt- und Meinungsforschung können personenbezogene Daten verwendet werden. Dies richtet sich nach § 30a BDSG und § 15 Abs. 3 TMG. Die Erlaubnisnorm für diesen Zweck ist wesentlich weiter gefasst als diejenige für Werbezwecke. Markt- und Meinungsforschung ist nach Ansicht des Gesetzgebers wesentliche Voraussetzungen für die nachhaltige demokratische und wirtschaftliche Entwicklung des Landes.[78]

Im Rahmen dieser Erlaubnisnorm ist eine Abwägung zu treffen. Ist ein schutzwürdiges Interesse eines Spielers an dem Ausschluss des Umgangs mit seinen personenbezogenen Daten erkennbar, so dürfen diese nicht verwendet werden, § 30a Abs. 1 BDSG. Werden personenbezogene Daten zum Zwecke der Markt- und Meinungsforschung erhoben, so sind diese gemäß § 30a Abs. 3 BDSG zu pseudonymisieren und sobald wie möglich zu anonymisieren. Diese Regelung gilt gemäß § 15 Abs. 3 Satz 1 und Abs. 5 Satz 3 TMG auch für die Verwendung von Nutzungsdaten durch Telemediendienstleister.

6.1.4 Verwendung personenbezogener Daten zum Zwecke der bedarfsgerechten Gestaltung von Telemedien

Ähnlich wie bei der Erlaubnisnorm zum Zwecke der Markt- und Meinungsforschung erlaubt es § 15 Abs. 3 TMG auch Nutzungsdaten zum Zwecke der bedarfsgerechten Gestaltung von Telemedien zu erheben, zu nutzen und zu speichern. Zu diesem Zweck dürfen aus den Nutzungsdaten Nutzungsprofile bei Verwendung von Pseudonymen erstellt werden. Generell gilt aber für die Erstellung von Nutzungsprofilen nach § 15 Abs. 3 TMG die Verpflichtung des Diensteanbieters, die personenbezogenen Daten zu pseudonymisieren und sobald wie mög-

[77] Roßnagel, in: NJW 2009, S. 2716 (2720).

[78] BT-Drs. 16/13657, S. 33.

lich zu anonymisieren. § 15 Abs. 3 TMG regelt auch, dass Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden dürfen. Außerdem besteht ein Widerspruchsrecht des Nutzers, auf das dieser hingewiesen werden muss.

6.1.5 Verwendung personenbezogener Daten mit dem berechtigten Interesse des Verantwortlichen und nicht überwiegendem schutzwürdigen Interesse des Betroffenen

Neben den aufgezählten Erlaubnisnormen für die Erhebung, Nutzung und Verarbeitung personenbezogener Daten findet sich eine weitere Zulässigkeitsnorm in Art. 7 lit. f) der EG-Datenschutzrichtlinie. Diese Norm kann von der Formulierung her als eine Art „Auffangerlaubnisnorm“ aufgefasst werden. Aufgrund ihrer Stellung in der Richtlinie ist aber davon auszugehen, dass diese Norm eine Datenerhebung, -nutzung oder -verarbeitung nicht erlaubt, wenn der Anwendungsbereich der speziellen Erlaubnisnormen eröffnet ist und diese spezielleren Normen keinen Erlaubnisgrund enthalten. Art. 7 lit. f) EG-Datenschutzrichtlinie hat einen von den anderen Erlaubnisnormen des Art. 7 EG-Datenschutzrichtlinie abzugrenzenden Anwendungsbereich.

Auch diese Norm ist in das deutsche Recht umgesetzt worden. § 28 Abs. 1 Satz 1 Nr. 2 BDSG erlaubt es nicht-öffentlichen Stellen, personenbezogene Daten zu eigenen Geschäftszwecken zu erheben, zu nutzen und zu verarbeiten, wenn dies zur Wahrung eines berechtigten Interesses der verantwortlichen Stelle erforderlich ist und kein Anlass zu der Annahme besteht, dass ein schutzwürdiges Interesse des Betroffenen dem entgegensteht bzw. das berechtigte Interesse überwiegt. Dieser Erlaubnistatbestand soll einen „Kompromiss im Widerstreit zwischen der informationellen Selbstbestimmung der Betroffenen und dem Informationsbedarf Dritter“ umschreiben.[79]

Die verantwortliche Stelle muss ihr berechtigtes Interesse grundsätzlich für den konkreten Sachverhalt und die konkreten personenbezogenen Daten nachweisen. Insoweit ist der Verwendungszweck klar zu formulieren und muss für den Betroffenen selbst und Dritte nachvollziehbar sein.[80] Weiterhin muss die Datenverwendung für die verantwortliche Stelle erforderlich sein. Dies ist dann der Fall, wenn es zu der speziellen Datenverwendung keine objektiv zumutbare Alternative gibt.[81] Für die Betreiber bedeutet dies, dass ihnen eine Datenverwendung auf Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG solange untersagt ist, wie sie ihre Informationsbedürfnisse anders befriedigen können. Erster Ansatzpunkt ist grundsätzlich die Erhebung von Daten bei dem Spieler selbst.

Eine verantwortliche Stelle kann eine Verwendung personenbezogener Daten nur dann auf ein berechtigtes Interesse stützen, wenn kein Grund zu der Annahme besteht, dass diese

[79] Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 28, Rn. 113.

[80] Gola / Schomerus, BDSG, 9. Auflage 2007, § 28, Rn. 34.

[81] Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 28, Rn. 143.

gegen ein überwiegend schutzwürdiges Interesse der Betroffenen verstößt. Insoweit hat vor der Datenverwendung eine Abwägung zwischen den berechtigten Interessen des Betreibers an der Verwendung der personenbezogenen Daten des Spielers und den schutzwürdigen Interessen des Spielers an seiner informationellen Selbstbestimmung zu erfolgen.[82] Dies kann im Ergebnis dazu führen, dass für bestimmte Verwendungsschritte ein berechtigtes Interesse des Betreibers an der Verwendung der personenbezogenen Daten des Spielers überwiegt und demnach zulässig ist, während in anderen Spielphasen und für andere Datenarten ein schutzwürdiges Interesse des Spielers an seiner informationellen Selbstbestimmung überwiegt. Eine Interessenabwägung hat in jeder Phase der Verwendung der personenbezogenen Daten konkret hinsichtlich der Situation und der jeweiligen verwendeten Daten zu erfolgen.

6.2 Verhältnis von Einwilligung und Vorliegen einer Zulässigkeitsnorm

Für den Publisher oder Betreiber von Online-Spielen ist in diesem Zusammenhang auch von Bedeutung, in welchem Verhältnis die beiden Erlaubnisalternativen – Einwilligung und Rechtsvorschrift – stehen. Dem Wortlaut nach stehen die beiden Alternativen gleichrangig nebeneinander. Dies würde bedeuten, der Betreiber eines Online-Spiels könnte sich aussuchen, auf welche Grundlage er die Datenverarbeitung stützt, wenn ihn eine Rechtsvorschrift ermächtigt und eine Einwilligung des Betroffenen vorliegt. Dem ist jedoch nicht so. Bei Einholung einer Einwilligung beim Spieler würde auch in Fällen des Vorliegens einer Rechtsvorschrift der Eindruck entstehen, dass die Datenerhebung, -nutzung und -verarbeitung von ihm beeinflusst werden könnte. Da aber auch bei Widerruf der Einwilligung, eine Datenerhebung, -nutzung und -verarbeitung zulässig wäre, würde dies zu einer Irreführung des Betroffenen führen. Es besteht für den Spieler keine Wahlfreiheit. Der Betreiber von Online-Spielen darf demnach auch aus Gründen der Rechtssicherheit eine Einwilligung, in Fällen in denen eine Erlaubnisnorm greift, nicht einholen, es sei denn, er will dem Spieler ein zusätzliches Widerrufsrecht einräumen.

6.3 Erlaubnisnormen für eine Übermittlung personenbezogener Daten in Drittstaaten

Ist eine Zulässigkeitsnorm für die Verwendung personenbezogener Daten gefunden oder liegt eine wirksame Einwilligung des Betroffenen in die Verwendung der Daten vor, so stellt sich im Zusammenhang mit der Nutzung von Internet und Online-Diensten ergänzend die Frage nach einer Zulässigkeit der Übermittlung der personenbezogenen Daten in Drittstaaten.

Hinsichtlich der Inhaltsdaten bildet Kapitel IV der EG-Datenschutzrichtlinie (Art. 25 und 26)

[82] Simitis, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 28, Rn. 130.

einen ersten Ansatzpunkt. Gemäß Art. 25 Abs. 1 EG-Datenschutzrichtlinie ist eine Übermittlung personenbezogener Daten in Drittstaaten zulässig, wenn der Drittstaat ein angemessenes Schutzniveau gewährleistet. Eine Übermittlung von personenbezogenen Daten in Drittstaaten, die kein entsprechendes Datenschutzniveau gewährleisten, ist nur zulässig, wenn auf anderen Wegen die Wahrung eines entsprechenden Datenschutzniveaus sichergestellt werden kann.

Ist ein Betreiber von Online-Spielen unsicher, ob eine Datenübermittlung von Inhaltsdaten in einen bestimmten Drittstaat zulässig ist, so sind zur Klärung Art. 25 Abs. 6 und 31 Abs. 2 EG-Datenschutzrichtlinie heranzuziehen. Danach kann die Kommission in einem förmlichen Verfahren feststellen, ob der jeweilige Drittstaat ein ausreichendes Datenschutzniveau erreicht. Diese Feststellung ist für die Mitgliedstaaten der Europäischen Union bindend. Die entsprechenden Feststellungen können auf der Webseite der Kommission eingesehen werden.[83] Sollen personenbezogene Daten in die USA übermittelt werden, ist es ergänzend möglich, eine Liste der US-amerikanischen Unternehmen einzusehen, die von sich behaupten, die sogenannten „Safe Harbor-Grundsätze“ einzuhalten und damit ein bestimmtes Datenschutzniveau zu gewährleisten.[84] Für diese Grundsätze hat die Europäische Kommission ein ausreichendes Schutzniveau im Sinne des Art. 25 Abs. 6 EG-Datenschutzrichtlinie anerkannt. Eine Übermittlung von personenbezogenen Daten an US-amerikanische Unternehmen, die diese Grundsätze gewährleisten, ist demnach zulässig.

In Bezug auf die Nutzungs- und Bestandsdaten sind für die Übermittlung dieser personenbezogenen Daten in Drittstaaten die Regelungen der §§ 12 ff. TMG heranzuziehen. Gemäß § 12 Abs. 2 TMG dürfen Telemediendiensteanbieter für eine Übermittlung von personenbezogenen Daten in Drittstaaten nicht auf die im BDSG enthaltenen Erlaubnistatbestände zurückgreifen. Insoweit bedarf es einer ausdrücklichen Erlaubnisnorm für die Übermittlung von Nutzungs- oder Bestandsdaten in Drittstaaten oder einer Einwilligung. Eine Einwilligung gemäß § 13 Abs. 2 TMG kann sich nach ausreichender Information des Spielers auch auf eine Übermittlung der personenbezogenen Daten in Drittstaaten beziehen.

Für die Übermittlung von Nutzungsdaten in Drittstaaten enthält § 15 Abs. 5 TMG eine Regelung. Danach dürfen Abrechnungsdaten durch einen Diensteanbieter an Dritte übermittelt werden. Die Übermittlung selbst muss zur Ermittlung des Entgelts und zur Abrechnung mit dem Spieler erforderlich sein. Anonymisierte Nutzungsdaten dürfen gemäß § 15 Abs. 5 Satz 3 TMG auch zum Zwecke der Marktforschung an andere Diensteanbieter übermittelt werden.

6.4 Rechte und Schutzmöglichkeiten der Online-Spieler

Publisher und Betreiber von Online-Spielen müssen nicht nur eine Erlaubnisnorm für die Verwendung personenbezogener Daten der Spieler nachweisen, sie müssen zusätzlich be-

[83] http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm.

[84] https://www.export.gov/safehrbr/list.aspx.

stehende Rechte der Spieler gewährleisten. Die wichtigsten Rechte von Spielern bei der Verwendung ihrer personenbezogenen Daten sind die Auskunfts-, Löschungs-, und Berichtigungsrechte. Diese Rechte ergeben sich aus den §§ 33 ff. BDSG und § 13 TMG. Der Spieler hat nach § 34 BDSG bzw. § 13 Abs. 7 TMG einen Auskunftsanspruch und nach § 35 BDSG bzw- § 13 Abs. 4 Nr. 2 TMG einen Löschungsanspruch. Dies beinhaltet auch das Recht auf Sperrung, wenn eine Löschung aus rechtlichen Gründen (z. B. Aufbewahrungspflichten) nicht möglich ist. Diese Rechte sind unabdingbar (§ 6 Abs. 1 BDSG).

Neben diesen Rechten haben Nutzer von Telemedien auch die Möglichkeit über die allgemein auch im BDSG aufgeführten Rechte hinaus, eine elektronische Einwilligung zu erteilen und zusätzliche technische und organisatorische Maßnahmen zu nutzen, die seine personenbezogenen Daten schützen, siehe § 13 Abs. 4, 6 TMG.[85] Gemäß § 13 Abs. 6 TMG sollen die Anbieter von Telemedien die Möglichkeit bereitstellen, diese anonym oder unter Pseudonym zu nutzen und die Beendigung der Nutzung eines Telemediendienstes zu jeder Zeit zu ermöglichen.

6.5 Ergänzende für Online-Spiele anwendbare Rechtsnormen

Neben dem BDSG, TMG und TKG sind im Rahmen einer vollständigen Betrachtung der anwendbaren Datenschutzbestimmungen für Online-Spiele ergänzend der Jugendmedienschutzstaatsvertrag (JMStV) für den Jugendschutz und Geheimhaltungsregelungen im StGB, der StPO und den berufsständischen Regelungen zu berücksichtigen. Hinzu kommen Aufbewahrungspflichten für insbesondere Rechnungsdaten im Rahmen der Abgabenordnung (AO) und des Handelsgesetzbuches (HGB). Diese werden in den einzelnen zu untersuchenden Funktionen von Online-Spielen im Folgenden punktuell aufgegriffen.

[85] Spindler / Nink, in: Spindler / Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 13 TMG, Rn. 8.

7 Analyse einzelner Berührungspunkte zwischen Datenschutzrecht und Online-Spielen

Im Folgenden werden die bisher gefundenen Ergebnisse miteinander in Verbindung gesetzt. Für konkrete Spielsituationen werden die einschlägigen Datenschutzbestimmungen aufgeführt und dargestellt. Dabei ist nicht nur zwischen den Spielsituationen zu unterschieden, sondern auch zwischen den einzelnen Akteuren. Es ist jeweils auf die verantwortliche Stelle abzustellen. Während in der Verkaufs- bzw. Vertriebssituation die personenbezogenen Daten in erster Linie für die Abwicklung eines Vertragsverhältnisses zwischen Publisher oder Händler und Online-Spieler anfallen und es sich in der klassischen Situation des Online-Verkaufs eines Spiels um Daten wie Name, Adresse, IP-Adresse und Bezahldaten handeln wird, fallen beim Betreiber sämtliche Informationen zum Spielverhalten, Spielverlauf, Video- und Tonsequenzen, aber eben auch Name, Pseudonyme, Bezahldaten, Adressen und IP-Adressen an.

7.1 Eröffnung des Anwendungsbereichs des Datenschutzrechts für die konkrete Spielsituation

Grundsätzlich kann nach dem oben Gezeigten zwischen einer Vielzahl von unterschiedlichen Fallkonstellationen im Rahmen der Datenerhebung, -nutzung und -verarbeitung bei Online-Spielen unterschieden werden. Ausschlaggebend für die Bestimmung des einschlägigen Datenschutzrechts ist die Niederlassung der verantwortlichen Stelle. Diese ist in der Regel der Betreiber des Online-Spiels. Zunächst wird daher nach den möglichen Niederlassungsorten einer verantwortlichen Stelle unterschieden. Dabei ist zu differenzieren zwischen solchen Fällen, in denen eine Niederlassung einer verantwortlichen Stelle in der Bundesrepublik Deutschland gelegen ist, im EU-Ausland oder in einem Drittstaat. Für Online-Spiele ist in diesem Zusammenhang jedoch zu beachten, dass es nicht ausschließlich auf die Spiele-Betreiber ankommt, sondern auch Spielsituationen zu berücksichtigen sind, in denen Dritte zur Weiterverarbeitung von personenbezogenen Daten von dem Betreiber in Anspruch genommen werden. Dies ist unter anderem dann der Fall, wenn der Betreiber die Abrechnung der Spiele, der Zusatzfunktionen usw. an einen Dritten abgibt. Vor dem Hintergrund der stetigen Zunahme von verteilten Systemen (Service Oriented Architectures, Cloud Computing) wird sich diese Problemstellung zudem in den kommenden Jahren weiter verschärfen.

7.1.1 Online-Spiele im privaten Bereich

Für alle Online-Spiele ist grundsätzlich zu berücksichtigen, dass datenschutzrechtliche Bestimmungen bei Datenverarbeitungen durch nicht-öffentliche Stellen zu ausschließlich per-

sönlichen oder familiären Zwecken nicht greifen, siehe § 1 Abs. 2 Nr. 3 und § 27 Abs. 2 Nr. 3 BDSG.[86] Was im Einzelnen als persönlich oder familiär anzusehen ist, richtet sich nach der Verkehrsanschauung.[87] Für Online-Spiele ist die Anwendung des BDSG insoweit ausgeschlossen, als die Datenerhebung, -verarbeitung oder -nutzung lediglich im privaten Aktionskreis zwischen einzelnen Spielern stattfindet und ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.[88] Ein Online-Spiel zwischen Familienmitgliedern, bei dem Daten erhoben werden, z. B. beim zusätzlich möglichen Chat, diese aber dem Publisher oder Betreiber nicht zur Verfügung gestellt werden, unterliegt daher nicht den Datenschutzbestimmungen des BDSG oder TMG. Jegliche nach außen gerichtete, über den persönlichen und familiären Kreis hinausgehende Tätigkeiten fallen jedoch in den Anwendungsbereich der Datenschutzgesetze.

7.1.2 Anwendbares Recht für Betreiber

Für Konstellationen, in denen personenbezogene Daten nur beim Spieler selbst erhoben werden und nur der Betreiber die erhobenen Daten verarbeitet oder nutzt, ist nach dem Sitz des Unternehmens bzw. dem Niederlassungssitz der verantwortlichen Stellen zu unterscheiden. Nach dem oben Dargestellten ist insoweit zwischen drei Standortvarianten zu unterscheiden: Sitz des Betreibers bzw. der tätigen Niederlassung in Deutschland, Sitz des Betreibers bzw. der tätigen Niederlassung in einem anderen Mitgliedstaat der Europäischen Union oder des EWR und Sitz des Betreibers in einem Drittstaat außerhalb der Europäischen Union.

7.1.2.1 Sitz der verantwortlichen Stelle (des Betreibers) in Deutschland

Sofern der Sitz der verantwortlichen Stelle und Erhebungs-, Verarbeitung,- oder Nutzungsort der personenbezogenen Daten in Deutschland belegen ist, findet das deutsche Datenschutzrecht und die entsprechenden spezialgesetzlichen Datenschutzbestimmungen Anwendung. Dies ergibt sich aus § 1 Abs. 2 BDSG und erstreckt sich gemäß § 1 Abs. 5 Satz 1, 2. Halbsatz BDSG auch auf alle Unternehmen, die Niederlassungen in Deutschland haben und hier die personenbezogenen Daten verwenden. Das BDSG orientiert sich damit am Territorialprinzip.[89] Liegen Sitz und Erhebungs-, Verarbeitungs- oder Nutzungsort der personenbezogenen Daten in Deutschland, gelten die Vorschriften des BDSG, siehe § 1 Abs. 2 BDSG. Der Betreiber von Online-Spielen mit Sitz in Deutschland unterliegt mithin gleichermaßen den Datenschutzbestimmungen des BDSG und des TMG, siehe §§ 3, 1 Abs. 5 TMG i. V. m. § 1 Abs. 5 BDSG.

---

[86] Siehe dazu Kapitel 5.1.3.

[87] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1, Rn. 151.

[88] Dammann, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 1, Rn. 150.

[89] Regierungsentwurf zum BDSG, in: BT-Drs. 14/ 4329, S. 31 f.

7.1.2.2 Sitz der verantwortlichen Stelle in der EU oder dem EWR

Für Diensteanbieter, die ihren Sitz in einem Mitgliedstaat der Europäischen Union oder im Geltungsbereich des EWR haben, findet das jeweilige nationale Datenschutzrecht Anwendung, siehe §§ 1 Abs. 5 BDSG, 3 Abs. 2 TMG. Es gilt das Herkunftslandprinzip, wonach es für den freien Verkehr von Waren und Dienstleistungen ausreichend ist, dass die entsprechenden Waren und Dienstleistungen im jeweiligen Mitgliedstaat zulässig sind.

Verfügt ein Diensteanbieter über eine Niederlassung im Bereich der Europäischen Union, so richtet sich das anwendbare Recht nach dem Ausübungsort seiner tatsächlichen und effektiven wirtschaftlichen Tätigkeit. Maßgeblich ist hierfür also der Schwerpunkt der wirtschaftlichen Tätigkeit[90], der jedoch nicht zwangsläufig der Standort der technischen Einrichtungen sein muss. Gleiches gilt auch im Bereich der Telemedien. Für die Online-Spiele-Betreiber ist demnach allein ausschlaggebend, wo der Schwerpunkt der Daten verwendenden Tätigkeit liegt. Betreiber innerhalb der Europäischen Union unterliegen daher nicht den verschiedenen Datenschutzgesetzen der 27 einzelnen Mitgliedstaaten, sondern lediglich denjenigen ihres Sitzlandes. Aufgrund des durch die EG-Datenschutzrichtlinie geschaffenen einheitlichen Schutzniveaus im Bereich des Datenschutzes wird den Rechten der Verbraucher in diesem Zusammenhang hinreichend Rechnung getragen.

Für den grenzüberschreitenden Datenverkehr innerhalb der EU knüpft § 1 Abs. 5 BDSG damit an das Sitzprinzip an, so dass für die Frage des anwendbaren Rechts nicht der physikalische Standort der Datenverarbeitung entscheidend ist. Dieses beruht auf der Vorstellung, dass es für den Binnenmarkt förderlich und für den Verbraucherschutz ausreichend ist, dass die entsprechenden Dienstleistungen im jeweiligen Mitgliedstaat den Vorgaben des koordinierten Rechts entsprechen. Nimmt der Betreiber datenschutzrelevante Handlungen über mehrere Niederlassungen vor, die in unterschiedlichen Mitgliedstaaten liegen, gilt für jede Niederlassung dasjenige Datenschutzrecht, in dem sich die jeweilige Niederlassung befindet, siehe Art. 4 Abs. 1 lit. a) Satz 2 EG-Datenschutzrichtlinie.

7.1.2.3 Sitz der verantwortlichen Stelle außerhalb der EU oder des EWR

Für Unternehmen mit Sitz in einem Staat außerhalb der Europäischen Union hingegen erlangt das deutsche Datenschutzrecht aufgrund der Regelung in § 1 Absatz 5 Satz 2 BDSG Anwendung; werden personenbezogene Daten in Deutschland erhoben, verarbeitet oder genutzt, so ist das BDSG anwendbar.

7.1.3 Konkrete Beispiele

Zusammenfassend lässt sich also feststellen, dass für Online-Spiele, soweit personenbezo-

[90] Erwägungsgrund 19 der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie).

gene Daten in Deutschland erhoben, genutzt oder verarbeitet werden oder der Betreiber eine Daten verwendende Niederlassung in Deutschland hat, deutsches Recht Anwendung finden wird. Je nach Art des Spiels, des Serverstandortes, der AGB des Betreibers, der Zahl der an dem Datenverarbeitungsprozess Beteiligten und der Art der Verbindung zum Betreiber ergeben sich hieraus die nachfolgenden denkbaren Fallgruppen.

7.1.3.1 Geschlossene Serversysteme (Server beim Betreiber oder dritten Dienstanbietern)

Zunächst soll die Situation bei geschlossenen Serversystemen dargelegt werden. Der folgende Beispielfall verdeutlicht die Problematik:

Die Firma A betreibt ein Online-Rollenspiel. Um hieran teilnehmen zu können, erwerben die Spieler eine Basissoftware und legen einen Account auf dem Spielserver an. Sie geben in einem Online-Formular ihre Kontaktdaten und Kreditkarteninformationen an. Beim Absenden des Online-Formulars werden die IP-Adresse des Spielers gespeichert und Cookies auf dem PC des Spielers abgelegt. Bevor die Spieler Zugang zu dem Spiel bekommen, müssen sie die Endbenutzerlizenzvereinbarungen (EULA) der Firma A akzeptieren. Darin heißt es:

Den Spielern ist es untersagt,

als Spielleiter die Software zu betreiben. Dies gilt insbesondere für die Initialisierung nicht autorisierter Spielserver über das Internet und lokale Gaming-Netzwerke;

auf eine nicht autorisierte Weise eine Verbindung zu dem Spielserver herzustellen.

Zur Vermarktung des Spiels betreibt die Firma A eine deutschsprachige Webseite, die unter einer deutschen Domain zu erreichen ist.

Der Spielserver der Firma A befindet sich

Fall 1: beim Sitz der Firma A in China.

Fall 2: beim Sitz der Firma A in Großbritannien.

Fall 3: beim Sitz der Firma A in Großbritannien. Die personenbezogenen Daten werden jedoch durch eine Niederlassung in Hamburg erhoben, verarbeitet und genutzt.

Welches Datenschutzrecht hat die Firma A zu beachten?

Anwendbares Recht für Fall 1:

Im Fall 1 befindet sich der Sitz der Firma A außerhalb der Europäischen Union. Für das anwendbare Datenschutzrecht in Deutschland sind demnach § 1 Abs. 5 BDSG und § 1 Abs. 5 TMG maßgeblich.[91] Die Firma A hat die deutschen Datenschutzbestimmungen des BDSG dann zu beachten, wenn sie personenbezogene Inhaltsdaten in Deutschland erhebt, verarbeitet oder nutzt, siehe §§ 1 Abs. 2, Abs. 5 Satz 2, 3 Abs. 3 BDSG.

[91] Siehe dazu Kapitel 5.1.3.

Erheben in diesem Sinne ist das Beschaffen von Daten über den Betroffenen, § 3 Abs. 3 BDSG. Vorliegend müssen die Spieler vor Beginn des Online-Spiels auf der Webseite der Firma A ein vom Unternehmen ausgestaltetes Online-Formular ausfüllen und absenden. Aufgrund der Sprache und der Ausgestaltung der Domain richtet sich das Angebot der Firma A gezielt an deutsche Nutzer. Solange der Spieler das zur Verfügung gestellte Online-Formular mit seinen personenbezogenen Daten ausfüllt, erhebt die Firma A bei dem Spieler aktiv keine personenbezogenen Daten.[92] Anders hingegen stellt sich die Situation hinsichtlich der gespeicherten IP-Adresse und der abgelegten Cookies dar. In diesem Fall wird die Firma A selbstständig aktiv tätig. Folglich erhebt die Firma A personenbezogene Daten beim Spieler. Das Unternehmen unterliegt daher den Vorschriften des BDSG, §§ 1 Abs. 2, Abs. 5, 3 Abs. 3 BDSG.

Hinsichtlich der Anwendbarkeit des TMG ist auf das Herkunftslandprinzip des § 3 Abs. 1 TMG zu verweisen. Soweit sich das Angebot jedoch an deutsche Spieler in deutscher Sprache richtet und eine deutsche Domain genutzt wird, ist nach der hier vertretenen Auffassung auch das TMG anwendbar.[93]

Anwendbares Recht für Fall 2:

Im Fall 2 ist die Firma A in Großbritannien ansässig. Sie unterliegt mit ihrem Angebot daher dem britischen Datenschutzrecht, § 1 Abs. 5 Satz 1 BDSG und § 3 Abs. 1 und 2 TMG.

Anwendbares Recht für Fall 3:

Etwas anderes gilt jedoch, wenn die Firma A personenbezogene Daten durch eine Niederlassung in Deutschland erhebt, verarbeitet oder nutzt. In diesem Fall muss die Firma A ihr deutsches Angebot an den Normen des BDSG und des TMG ausrichten, siehe § 1 Abs. 5 Satz 1, 2. Hs. BDSG und § 3 Abs. 1 TMG. Die Firma A würde eine solche Niederlassung betreiben, wenn sie ihre wirtschaftliche Tätigkeit effektiv und tatsächlich von Deutschland aus erbringt. Dies wäre anzunehmen, wenn die Firma A ihr Spiel für den deutschen Raum von einem Büro in Deutschland aus vermarktet und organisiert. Der tatsächliche Standort des Servers wäre dann unerheblich; es gilt das Niederlassungsprinzip bzw. Herkunftslandsprinzip.

7.1.3.2 Offene Serversysteme (Server vom Betreiber des Online-Spiels unabhängig)

Eine andere Bewertung kann sich bei offenen Serversystemen ergeben. Die rechtliche Bewertung bei sogenannten offenen Serversystemen, also solchen Systemen, bei denen der

[92] Siehe dazu ausführlich Kapitel 5.2.2.

[93] Siehe dazu Kapitel 5.2.2.

Server vom Betreiber des Online-Spiels unabhängig ist, wird an weiteren Beispielen erläutert:

7.1.3.2.1 Online-Spiele auf dem PC

Das Online-Spiel A wird als DVD-Version vertrieben. Nachdem die Spieler die Software auf ihrem PC installiert haben, können sie gegen die von ihrem Computer gesteuerten Gegner kämpfen. Zusätzlich weist das Spiel die Möglichkeit eines integrierten Mehrspielermodus auf. Mit diesem bauen die Spieler eine Verbindung zu einem Spielserver auf und können nun gegen andere Spieler antreten. Einen solchen Server kann jeder Spieler mit Hilfe der Spielsoftware im Internet oder einem privaten LAN bereitstellen.

Welche Datenschutzregelungen finden in den folgenden Fällen Anwendung?

Fall 1:

Bevor der Spieler eine Verbindung zu einem sich im Internet befindenden Server herstellen kann, muss er sich auf der Website des Herstellers registrieren, um das mitgelieferte Verbindungstool frei schalten zu können. Dieses wird vom Hersteller auf den PC des Spielers abgelegt. Ist dies geschehen, listet das Tool zum einen die erreichbaren Server auf. Zum anderen überprüft es, ob die vom Spieler verwendete Version aktuell und registriert ist. Die Aktualisierung der Software erfolgt ausschließlich über das Tool. Hiernach stellt das Tool die Verbindung zum Server her. Das Tool wiederum stellt einen „eigenen“ Server dar, da sämtliche interaktiven Aktivitäten der Spieler ausschließlich über die Webseite des Tools abrufbar und spielbar sind.

Fall 2:

Möchte der Spieler das Spiel in einem in Eigenverantwortung betriebenen LAN als Privatperson spielen, wird das Verbindungstool deaktivieren bzw. nicht genutzt, so dass kein Abgleich der Daten über das Internet stattfindet. Sodann spielen die Spieler im Rahmen des privaten LAN miteinander; es ist jedoch zuvor eine Registrierung in Gestalt des Einloggens über den Server erforderlich.

Fall 3:

Zwei Spieler wollen das Spiel über das Internet spielen und nutzen hierbei einen der PCs der Spieler als privaten Server. Eine Anmeldung über den Server des Publishers / Online-Spiel-Betreiber erfolgt nicht.

Anwendbares Recht für Fall 1:

Im Fall 1 muss der Spieler das Verbindungstool verwenden, um online spielen zu können. Neben der Verbindung zum gewählten Spielserver baut dieses Tool eine weitere Verbindung zum Server des Betreibers auf. Hierdurch hat der Spieler die Gewissheit, stets die aktuelle Software installiert zu haben. Weiterhin erhält der Spieler einen vereinfachten Überblick über die erreichbaren Server, so dass er sich nicht mit der Netzwerktechnik selber auseinandersetzen muss. Schließlich kann auch der Betreiber auf diese Weise prüfen, ob die jeweils genutzte Version lizenziert ist. Rechtlich lässt sich dies dergestalt einordnen, dass zunächst

von einer Datenerhebung und -verarbeitung durch den Betreiber auszugehen ist. Da sich diese gezielt an Spieler in Deutschland richtet und auf dem PC des Spielers die entsprechenden Installationsdateien abgelegt werden, kommt deutsches Datenschutzrecht in Gestalt insbesondere des BDSG und TMG zur Anwendung.

An dieser rechtlichen Einordnung ändert sich auch nichts, wenn der Spielserver in einem Drittland steht, da durch die stets erforderliche Zwischenschaltung des Verbindungstools und dessen Webserver zur Einwahl eine Datenerhebung im Inland erfolgt. Auch in diesem Fall bleibt der Online-Spiele-Betreiber verantwortlich für die erhobenen und verarbeiteten personenbezogenen Daten.

Anwendbares Recht für Fall 2:

Im Fall 2 ist ein Einloggen über den Server des Toolanbieters erforderlich, bevor die Spieler im LAN-Modus miteinander spielen können, ohne den Toolserver bzw. ohne den Spieleserver zu nutzen, zu dem der Toolserver verlinkt hat. Insoweit ist entsprechend den Ausführungen zum Fall 1 der Anbieter des Tools verantwortlich Stelle bzgl. der durch ihn erhobenen Daten. Es kommt daher im Verhältnis Spieler – Betreiber deutsches Datenschutzrecht zur Anwendung. Im Verhältnis der Spieler innerhalb des LAN erfolgt keine Datenerhebung bzw. Datenverarbeitung, die über eine rein persönliche Tätigkeit i. S. d. § 1 Abs. 2 Nr. 3 BDSG hinausgeht. Aus diesem Grund ist das BDSG im Verhältnis der Spieler untereinander in der Regel nicht anwendbar. Im TMG findet sich keine zum § 1 Abs. 2 Nr. 3 BDSG vergleichbare Regelung. Jedoch schließt § 11 Abs. 1 TMG die Anwendbarkeit der Datenschutzvorschriften des TMG aus für Dienste im Dienst- und Arbeitsverhältnis, wenn die Datenverarbeitung zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt. Dies muss dann erst recht für den rein privaten Bereich gelten, wenn es sich um ein geschlossenes Netzwerk handelt.

Anwendbares Recht für Fall 3:

Verarbeitet und genutzt werden in diesem Zusammenhang in erster Linie die IP-Adressen der Spieler und weitere Login-Informationen bzw. Spieldaten. Insoweit ist deutsches Datenschutzrecht anwendbar, wenn sich der Betreiber des PCs in Deutschland befindet, § 1 Abs. 2 BDSG bzw. § 3 TMG. Allerdings dürfte es sich auch hier in der Regel um eine ausschließlich persönliche Tätigkeit handeln, so dass die Datenschutzgesetze keine Anwendung finden.

7.1.3.2.2 Online-Spiele auf Spielkonsole

Das Spiel A wird auf einer Spielkonsole gespielt, der Spieler spielt in Deutschland und hat dort seinen gewöhnlichen Aufenthaltsort.

Welches Datenschutzrecht findet Anwendung?

Zunächst ist zu klären, worin sich Spielkonsolen von anderen Spielsystemen unterscheiden. Spielkonsolen werden üblicherweise in Online-Netzwerken betrieben, deren Zugang über das Internet erfolgt und die vom Hersteller der Konsole betrieben werden (z. B. Xbox Live, PSN, Wii Connect). Sie umfassen verschiedene Funktionen, die je nach Zugangsart zur Ver-

fügung stehen. In der teilweise noch kostenfreien Version, in der bereits im Zuge der Anmeldung personenbezogene Daten des Spielers erhoben und gespeichert werden, hat der Spieler bereits Zugriff auf einzelne zusätzliche Komponenten wie die Community, Teile des sogenannten Marktplatzes und Demo-Trailer. In der kostenpflichtigen Version (etwa bei Xbox Live Gold) hingegen hat der Spieler uneingeschränkten Zugriff auf Komponenten wie Videochat, Marktplatz und die Mehrspielerunterstützung, d. h. erst im kostenpflichtigen Modus ist auch ein Online-Spielen gegen bzw. mit anderen Spielern möglich[94]. Der Server und die gesamte Infrastruktur (außer des Zugriffs über das Internet) für die Spieler werden von dem Spielsystembetreiber (z. B. Microsoft, Sony, Nintendo) direkt gestellt. Insoweit handelt es sich beim Spielkonsolen-Netzwerk um ein zentralisiertes Netzwerk.

Verantwortlich für die Erhebung und Verwaltung der Daten, die für die Verwaltung des Spielsystems anfallen, ist grundsätzlich der Betreiber des Spielsystems. Da im Rahmen der Netzwerkbereitstellung personenbezogene Daten erhoben und verarbeitet werden, der Spieler sich in Deutschland befindet und sich das Spielsystem ausdrücklich an Deutsche richtet, kommt das deutsche Datenschutzrecht in diesem Fall zur Anwendung. Etwas anderes gilt nur, wenn der Betreiber des Spielsystems keine Niederlassung in Deutschland hat, sondern nur in der EU / dem EWR. Dann würde das Recht dieses Staates gelten.

Der Betreiber des konkreten Online-Spiels selbst kann ebenfalls verantwortliche Stelle sein hinsichtlich der konkret im Spiel anfallenden Daten. Dies ist insbesondere der Fall, wenn er eigene Server zusätzlich zu dem Spielsystem bereitstellt. Doch auch für sonstige Spiele-Betreiber kann dieses gelten, da sie in der Regel nach Start des Spiels für den Spieler als Daten verarbeitende Stelle unter Nutzung der Infrastruktur des Spielsystems auftreten. Eine Auftragsdatenverarbeitung durch den Betreiber des Spielsystems im Auftrag des Spiel-Betreibers scheidet in der Regel allerdings aus, da der Betreiber des Spielsystems eigene kommerzielle Interessen mit dem Dienst verfolgt. Im Einzelfall ist somit stets für jede Phase der Datenverarbeitung abzugrenzen, welche Stelle gerade verantwortlich dafür ist.

Hinsichtlich des anwendbaren Rechts gilt das schon zu den Spielsystemen gesagte, da durch die Regionalkontrolle der Spielsysteme für jedes Land nur die Spiele freigeschaltet werden, an die es sich ausdrücklich richtet. In Deutschland dürfte somit auch hier in der Regel deutsches Datenschutzrecht Anwendung finden, sofern nicht der Betreiber seine Niederlassung nur EU / EWR-Ausland hat.

7.1.3.2.3 Drei- und Mehrparteien-Konstellationen – Auftragsdatenverarbeitung

Der Kommunikations- und Datenfluss in Konstellationen mit drei oder mehr Beteiligten kann zu anderen Voraussetzungen und damit zu anderen rechtlichen Bewertungen führen als in Konstellationen mit lediglich zwei Beteiligten.

Bei Konstellationen mit drei oder mehr Beteiligten ist zu differenzieren, auf welche Weise und

[94] PSN und Wii-Connect erheben z. Zt. keine monatlichen Gebühren.

von woher der Datenfluss wohin geschieht, wo die Datenverarbeitung erfolgt und insbesondere wer verantwortliche Daten verarbeitende Stelle ist. Insoweit ist zu differenzieren zwischen einer Datenverarbeitung zu eigenen Zwecken des Verarbeiters und einer Auftragsdatenverarbeitung. Ein Auftragsdatenverarbeiter ist gemäß Art. 2 lit. e) EG-Datenschutzrichtlinie eine juristische oder natürliche Person, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet (vgl. auch § 3 Abs. 7 2. Alt. BDSG). Stellt die Verarbeitung der personenbezogenen Daten das wesentliche Element der Aufgabenübertragung dar und ist der Auftragnehmer lediglich in Hilfs- und Unterstützungsfunktion für den Vertragspartner tätig, so ist grundsätzlich bei Vorliegen der sonstigen Anforderungen des § 11 BDSG von einer Auftragsdatenverarbeitung auszugehen.[95]

Liegt eine Auftragsdatenverarbeitung vor, so ist nicht der Auftragnehmer, sondern der Auftraggeber für die Einhaltung der gesetzlichen Datenschutzbestimmungen verantwortlich. Der Auftraggeber hat die Pflicht, den Auftragnehmer sorgfältig auszusuchen und sich von der Einhaltung der gesetzlichen Vorschriften zu überzeugen; der Auftragnehmer hingegen hat die Datenverarbeitung nach den Weisungen des Auftraggebers durchzuführen und die für die Durchführung erforderlichen technisch-organisatorischen Maßnahmen sicherzustellen.[96]

Bei Online-Spielen sind solche Konstellationen insbesondere dann relevant, wenn Betreiber externe Services wie Rechenzentren, Spielsysteme oder sogar das Management des Spiels in Anspruch nehmen. Folgende Fallkonstellationen sind denkbar:

Fall 1: Der Auftraggeber ist in der EU ansässig, der Auftragnehmer im Drittland.

Bei dieser Konstellation ist der für die personenbezogenen Daten verantwortliche Auftraggeber in der EU ansässig, daher gelten die Datenschutzbestimmungen desjenigen Mitgliedstaates, in dem der Auftraggeber ansässig ist. Hierbei ist jedoch zu beachten, dass die Privilegierung der Auftragsdatenverarbeitung nach § 11 BDSG nur für Stellen gilt, die in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen (§ 3 Abs. 8 Satz 3 BDSG). Für verantwortliche Stellen außerhalb der EU sind die Vorschriften über die Auftragsdatenverarbeitung somit direkt nicht anwendbar. Die Weitergabe von personenbezogenen Daten stellt dann eine Übermittlung dar, deren Zulässigkeit nach den §§ 27ff. BDSG i. V. m. § 4b und § 4c BDSG zu beurteilen ist. Allenfalls könnte bei entsprechend detaillierter vertraglicher Gestaltung noch eine Übermittlung zur Wahrung berechtigter Interessen i. S. d. § 28 Abs. 1 Nr. 2 BDSG angenommen werden. Dies ist jedoch nicht für den Bereich der Telemedien und somit nicht für Nutzungsdaten und Bestandsdaten bei Online-Spielen möglich.

---

[95] Walz, in: Simitis (Hrsg.), BDSG, 6. Auflage 2006, § 11, Rn. 16.

[96] Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau / Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau, SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, 2007, S. 17.

Fall 2: Auftraggeber und Auftragnehmer sind in der EU ansässig, ein Unterauftragnehmer ist im Drittland ansässig.

Grundsätzlich ist die Beauftragung eines Unterauftragnehmers dann zulässig, wenn dieses ausdrücklich zwischen Auftraggeber und Auftragnehmer vereinbart worden ist. Wie bei Fall 1 gilt jedoch, dass ein Standartvertrag zwischen dem Auftragnehmer in der EU und dem Unterauftragnehmer im Drittland nicht im Rahmen der Auftragsdatenverarbeitung zulässig ist. Der Auftragnehmer (ggf. in Zusammenwirkung mit dem Auftraggeber) ist als Datenexporteur i. S. d. §§ 4b, 4c BDSG einzustufen, der Unterauftragnehmer als Datenimporteur.

Fall 3: Ein in der EU ansässiger Auftraggeber beauftragt einen Auftragnehmer in einem Drittstaat, dieser Auftragnehmer bedient sich eines weiteren Auftragnehmers in der EU, der die Daten an das Unternehmen zurück übermittelt.

Eine Besonderheit in dieser Konstellation ist, dass der (zweite) Auftragnehmer in der EU seine Daten vom (ersten) Auftragnehmer in einem Drittstaat erhält; ein Vertrag besteht also nur zwischen dem in der EU ansässigen Unternehmen und dem (ersten) Auftragnehmer in einem Drittstaat. Rechtlich hat dies zur Folge, dass Zweck und Umfang der zulässigen Datenverarbeitung sowie die einzuhaltenden Datensicherheitsmaßnahmen in dem Vertrag zwischen dem in der EU ansässigen Auftraggeber und dem (ersten) Auftragnehmer in einem Drittstaat zu bestimmen sind.

Fall 4: Ein in einem Drittland ansässiger Auftraggeber beauftragt einen in der EU ansässiger Auftragnehmer, in der EU personenbezogene Daten zu erheben und diese an den Auftraggeber zu übermitteln

In diesem Fall ist der Auftragnehmer für die von ihm durchgeführte Datenverarbeitung verantwortlich, siehe Art. 17 EG-Datenschutzrichtlinie, § 11 BDSG i. V. m. § 9 BDSG. Bei der weiteren Verarbeitung ist der Auftraggeber im Drittland selbst verantwortlich. Der Auftragnehmer hat selbst keine Verantwortung im Sinne der §§ 4b, 4c BDSG. Würde man eine solche annehmen, so müsste der Auftragnehmer eine umfassende Prüfung der gesamten Datenverarbeitung vornehmen. Der Auftraggeber wird hier aber nur einen kleinen Ausschnitt der Datenverarbeitung und des Verwendungszusammenhangs kennen; die Rechtmäßigkeit der Verarbeitung von Daten im Konzernzusammenhang wird er nicht beurteilen können. Insofern dürfte es für den Auftragnehmer in der EU in den meisten Fällen unmöglich sein, eine umfassende Prüfung im Sinne der §§ 4b, 4c BDSG vorzunehmen, um beurteilen zu können, ob eine Katalogausnahme gegeben ist.[97] Mithin trifft den Auftragnehmer in der EU keine Verantwortung im Sinne der §§ 4b, 4c BDSG. Gemäß § 1 Abs. 5 BDSG liegt die Verantwortung für die Vereinbarkeit der Datenverarbeitung mit den bestehenden Regelungen bei der verantwortlichen Stelle im Drittstaat.[98] Es könnte ihn jedoch eine Remonstrationspflicht ge-

[97] Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung der Fallgruppen zur internationalen Auftragsdatenverarbeitung, S. 16.

[98] Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung der Fallgruppen zur internationalen Auftragsdatenverarbeitung, S. 16.

mäß § 11 Abs. 3 Satz 2 BDSG treffen. Er müsste den Auftraggeber unverzüglich auf eine mögliche Rechtsverletzung hinweisen.[99]

Fall 5: Ein in der EU ansässiger Auftragnehmer wird von einem Auftraggeber aus einem Drittstaat beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu übermitteln; die Daten wurden vom Auftraggeber in der EU erhoben.

In dieser Konstellation wird die Dienstleistung des Auftragnehmers in der Regel darin bestehen, eine Rechenzentrumsdienstleistung zu erbringen. Deshalb ist eine inhaltliche Kenntnisnahme der Daten durch den Auftragnehmer hier typischerweise nicht vorgesehen; der Auftragnehmer hat lediglich für die Datensicherheit zu sorgen. Sollte dem Auftragnehmer jedoch bekannt werden, dass die Datenverarbeitung gegen das BDSG verstößt, hat er auch in diesem Fall eine Remonstrationspflicht nach § 11 Abs. 3 Satz 2 BDSG. Dies trifft auch auf die Fälle zu, in denen dem Auftragnehmer bekannt wird, dass offensichtlich kein ausreichendes Datenschutzniveau beim Auftraggeber besteht und kein Ausnahmetatbestand im Sinne des § 4c Abs. 1 BDSG erfüllt ist. Hieraus kann sich unter Umständen eine Verpflichtung des Auftragnehmers ergeben, die weitere Ausführung des Auftrags einzustellen.[100]

Fall 6: Ein in der EU ansässiger Auftragnehmer wird von einem Auftraggeber aus einem Drittstaat beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber zu übermitteln; die Daten wurden vom Auftraggeber in einem Drittstaat erhoben.

Unter der Annahme, dass die Daten aus dem Drittstaat nach dortigem Recht zulässig erhoben werden, ist gemäß § 1 Abs. 5 Satz 2 BDSG das BDSG auch anzuwenden, wenn die verantwortliche Stelle personenbezogene Daten in Deutschland verarbeitet oder nutzt.

Fall 7: Ein in der EU ansässiger Auftragnehmer wird von einem Auftraggeber aus einem Drittstaat beauftragt, personenbezogene Daten zu verarbeiten und danach an den Auftraggeber in verschlüsselter Form zu übermitteln; die Daten wurden vom Auftraggeber in einem Drittstaat erhoben.

Bei dieser Fallkonstellation muss der Auftraggeber die Regelungen des BDSG nicht berücksichtigen, da die Konstellation mit der in § 1 Abs. 5 Satz 4 BDSG normierten Transitregelung vergleichbar ist. Die Daten werden in diesem Fall nur durch das Gebiet der Europäischen Union durchgeführt, sie werden hier weder erhoben, verarbeitet noch genutzt. Darüber hinaus besteht auch keine weitere Verantwortlichkeit des Auftragnehmers. Vielmehr lässt sich hier konstatieren, dass materielles deutsches Datenschutzrecht nicht gilt, wenn der Auftragnehmer nicht auf die vom Auftraggeber übermittelten Daten zugreifen kann.

---

[99] Wedde, in: Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 11, Rn. 65.

[100] Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung der Fallgruppen zur internationalen Auftragsdatenverarbeitung, S. 17.

Fall 8: Ein Spieler nutzt im Rahmen eines Online-Spiels die Möglichkeit einer VoIP-Software und kommuniziert mit den Mitspielern. Weitere Spieler, die gleichzeitig das Spiel online spielen und die Möglichkeit der VoIP-Software nutzen, befinden sich in der EU und in einem Drittland.

Die VoIP-Software ermöglicht es den Spielern, via Internet oder LAN miteinander zu kommunizieren. Jeder VoIP-Server ist in Räume, sogenannte Channels, unterteilt; je nach Serverkonfiguration können die Spieler auf einem Server neue Räume eröffnen und auf Wunsch per Passwort schützen. Je nach Server können hier die Einstellungen variieren. Die Software wird jeweils vom einzelnen Spieler auf seinen PC heruntergeladen. Die Kommunikation mit Hilfe der VoIP-Software unterliegt dem Datenschutzrecht (insbesondere auch dem Fernmeldegeheimnis) des Staates, in dem der Spieler ansässig ist.

Zusammenfassung

Zusammenfassend lässt sich also festhalten, dass bei Konstellationen mit drei oder mehr Beteiligten in der Regel ebenfalls deutsches Datenschutzrecht Anwendung findet. Entsprechend der jeweiligen Konstellation eines Online-Spiels kann auch nationales Recht der Mitgliedstaaten Anwendung finden.

8 Datenschutzrechtliche Erläuterungen

Im Folgenden werden die aus Datenschutzsicht wichtigsten Funktionalitäten von Online-Spielen betrachtet und detaillierter untersucht. Die folgenden Ausführungen konzentrieren sich auf die Rechtsfragen, die entweder für alle Funktionen von Bedeutung sind oder die nur für einzelne Funktionen besondere Relevanz haben.

8.1 Grundsätzliches

Grundsätzlich sind von den Online-Spiele-Betreibern die einschlägigen Datenschutzbestimmungen zu berücksichtigen, vorliegend in erster Linie die Regelungen des TMG und des BDSG. Das BDSG findet nur dann Anwendung, wenn das TMG keine spezielleren Regelungen für den Umgang mit personenbezogenen Daten, die zur Bereitstellung von Telemedien verwendet werden, enthält.[101]

Neben der Rechtmäßigkeit der Verwendung personenbezogener Daten sind die Hersteller, Publisher und Betreiber von Online-Spiele auch an die Grundsätze der Zweckbindung, Erforderlichkeit, Transparenz und der Datensicherheit gebunden. Im Sinne des Erforderlichkeitsgrundsatzes müssen Hersteller, Publisher und Betreiber von Online-Spielen in jeder Phase einer Spielentwicklung identifizieren, welche Daten anfallen, in welchem Prozess sie anfallen und ob sie für diesen Prozess bzw. den weiteren Verlauf erforderlich sind. Anhand dieser Ergebnisse ist dann für die jeweils anfallenden Daten erneut zu überprüfen, ob sich eine Erlaubnisnorm finden lässt bzw. eine Einwilligung vorliegt. Nur die personenbezogenen Daten, für die eine Einwilligung oder eine Erlaubnisnorm für die Erhebung, Verarbeitung oder Nutzung vorliegt, dürfen dann entsprechend den jeweiligen gesetzlichen Vorgaben verwendet werden.

So ist es unter anderem über den gesamten Zeitraum der Nutzung eines Telemediendienstes – also bis zum Beenden des Spiels durch Ausloggen o. ä. – technisch erforderlich, die IP-Adresse des Spielers von Online-Spielen zu verwenden, da anderenfalls eine Adressierung der angeforderten Spielseiten nicht möglich wäre. Über die Nutzung des Spiels hinaus wird eine Speicherung dieser Daten jedoch zumeist nicht erforderlich sein, da das Datum selbst für die Abrechnung des genutzten Spiels oder weitergehende Phasen nicht notwendig ist. Für kostenlose Spiele werden unter anderem die Dauer und der Umfang der Nutzung keiner Speicherung bedürfen, da eine Abrechnung gerade nicht erfolgt. Die Daten sind mithin nicht erforderlich.

Für anderweitig technisch bedingt anfallende personenbezogene Daten ist zu berücksichtigen, dass es sich bei dem Vorgang des „Anfallens“ nicht um ein Erheben im Sinne der deut-

[101] Siehe dazu Kapitel 5.4.

schen Datenschutzbestimmungen handelt. Gemäß § 3 Abs. 3 BDSG, welcher aufgrund des Fehlens einer eigenen Legaldefinition im TMG auch auf Telemedien Anwendung findet, werden Daten nur dann erhoben, wenn sie aktiv und zielgerichtet beschafft werden. Bei zufällig anfallenden Daten bzw. aufgedrängten Daten sind technisch-organisatorische Maßnahmen zu treffen, dass diese gerade nicht gespeichert werden und zu einer späteren Nutzung oder Verarbeitung eventuell zur Verfügung stehen würden.

8.2 Personenbezug

Sind die bei den einzelnen Prozessen und Spielphasen anfallenden Daten identifiziert, ist für jedes einzelne Datum bzw. die Kombination dieser Daten der Personenbezug zu untersuchen. Dieser Personenbezug kann in den einzelnen Phasen insbesondere für Nutzernamen, IP-Adressen, Protokoll- und Log-Dateien unterschiedlich beurteilt werden.

Fraglich ist insoweit, ob es sich bei Nutzernamen, die keinen Bezug zum Realnamen aufweisen, um ein personenbezogenes Datum handelt. Für die meisten Online-Spiele ist es erforderlich, dass sich der Spieler beim Betreiber des Spiels anmeldet. Wählt er ein Pseudonym, das keine Bestandteile des realen Namens des Nutzers enthält, ist ein direkter Bezug zu seiner Person durch diejenigen, die keinen Zugang zu den weiteren Anmeldedaten haben, nicht möglich. Es liegt ein relativer Personenbezug vor, bei dem weiterhin die Datenschutzgesetze anwendbar sind. Es bestehen jedoch erweiterte Verarbeitungsmöglichkeiten für diese pseudonymisierten Daten (z. B. § 15 Abs. 3 TMG). Der Betreiber des Online-Spiels, der Zugang zu den Anmeldedaten hat, kann mit Hilfe dieser den Spieler bestimmen und einen direkten Personenbezug herstellen. Insoweit ist auch für den Betreiber das TMG bzw. das BDSG anwendbar.

Nicht von den Datenschutzgesetzen erfasst sind anonyme, also nicht personenbezogene, Daten. Liegen Daten mit Personenbezug vor, kommt eine Anonymisierung dieser Daten in Frage: Entsprechend dem Wortlaut des § 3 Abs. 6 BDSG sind anonymisierte Daten derart verändert, dass die ehemals bestehenden Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten Person zugeordnet werden können.

Von besonderer Bedeutung im Zusammenhang mit Online-Spielen sind die IP-Adressen, die E-Mail-Adressen der Spieler und die auf dem PC hinterlassenen Cookies.

Ob es sich bei diesen Daten um personenbezogene Daten handelt, ist umstritten.[102] Es ist auch in diesem Zusammenhang danach zu fragen, ob die jeweiligen Adressen einen Rückschluss auf die dahinter stehende Person zulassen. Für E-Mail-Adressen mit Namensbestandteilen ist dieses möglich. Bei E-Mail-Adressen ohne Namensbestandteile, IP-Adressen und Cookies lässt sich ein Personenbezug nur über Zusatzwissen herstellen.

[102] Siehe dazu exemplarisch: Heckmann, in: juris PK-Internetrecht, Kapitel 1.12, Rn. 20ff.

IP-Adresse

Eine IP-Adresse erlaubt es, den Zugriff auf einen Internetdienst einem bestimmten Internetanschluss zuzuordnen. Die IP-Adressen werden jeweils vom Access-Provider vergeben. Im Falle der IP-Adressen ist zu unterschieden zwischen IP-Adressen, die bei jeder Einwahl in das Internet neu vergeben werden (dynamische IP-Adressen) und solchen, die fest einem Anschluss zugeordnet sind (statische IP-Adressen).[103] Die dynamischen IP-Adressen sind in der Regel zwar nicht direkt durch den Spiele-Betreiber auflösbar, da sie sich bei jeder Einwahl ändern und der jeweilige Spieler jedes Mal eine neue IP-Adresse zugewiesen bekommt. Für den Access-Provider, der die dynamischen IP-Adressen dem Nutzer zuweist, sind diese jedoch bestimmbar und daher auch personenbeziehbar. Die Auflösung ist beim Zusammenspiel von Provider und Spiele-Betreiber unmittelbar möglich. Daher geht die herrschende Meinung davon aus, dass auch dynamische IP-Adressen zumindest personenbeziehbar sind und damit die Datenschutzgesetze anwendbar sind. Dies muss dann erst recht für statische IP-Adressen gelten.

E-Mail-Adresse

Hinsichtlich der E-Mail-Adressen mit nachvollziehbaren Namensbestandteilen liegt unmittelbar ein Personenbezug vor. Aber auch für E-Mail-Adressen die sich im Internet mit weiteren Informationen kombinieren lassen und so einer bestimmten Person zuordnen lassen, ist ein Personenbezug gegeben. Dies gilt für den Spiele-Betreiber und E-Mail-Provider auch, wenn er selbst über die erforderlichen Informationen verfügt, die für die Personenbeziehbarkeit notwendig sind. Allerdings ist der E-Mail-Provider nicht verpflichtet, den Nutzer eindeutig zu identifizieren.

Bei E-Mail-Adressen, die keinen Namensbestandteil enthalten und in auch nicht auf anderer Art und Weise mit weiteren Daten kombiniert werden können, könnte ein Personenbezug verneint werden. Das TMG wäre in derartigen Fällen somit nicht anwendbar. Allerdings kann technisch nicht unterschieden werden zwischen E-Mail-Adressen, deren Inhaber mit verhältnismäßigem Aufwand identifizierbar ist und solchen, für die solche Daten nicht erreichbar sind. Außerdem wäre eine Auflösung des Inhabers der E-Mail-Adresse zumindest durch den Inhaber selber möglich, so dass zumindest von einem Pseudonym auszugehen ist und damit die Datenschutzgesetze einschlägig sind.

Cookies

Cookies werden in der Regel dann auf dem Rechner des Spielers gespeichert, wenn er den Server des jeweiligen Betreibers besucht und er das Setzen von Cookies nicht durch entsprechende Einstellungen (z. B. im Browser) unterbunden hat. Bei einem Cookie handelt es sich um einen Datensatz, der auf dem Rechner des Online-Spielers gespeichert wird. Diese Datensätze enthalten in der Regel Zeichenreichen, die der Betreiber als Kennung des Rech-

[103] Siehe dazu: https://www.datenschutzzentrum.de/ip-adressen.

ners verwendet, um mehrere Aktionen des Nutzers miteinander in Beziehung zu setzen. Cookies werden beispielsweise für das Füllen von Warenkörben beim E-Shopping eingesetzt, damit der Nutzer bei den verschiedenen Schritten seines Einkaufs wiedererkannt werden kann. Im Bereich der Online-Spielen können die Betreiber auf ihren Servern zu den eindeutigen Kennungen ihrer Spieler (bzw. deren Rechner) Informationen zu deren Surfverhalten speichern. So kann beispielsweise nachverfolgbar gemacht werden, welche Webseiten des Betreibers der Spieler besucht oder welche Dienste er in Anspruch genommen hat. Zu unterscheiden ist zwischen dynamischen bzw. Session-Cookies und statischen bzw. persistenten Cookies. Während sich die Lebensdauer von Session-Cookies ausschließlich auf den jeweils aktuellen Besuch einer Webseite erstreckt und damit der Betreiber auch nur für diese Dauer Profile über das Surfverhalten erstellen kann, ermöglichen persistente Cookies, dass der Betreiber Daten über das Surfverhalten des Nutzers über einen längeren Zeitraum mitführt und auswertet. Wenn damit verbunden ist, dass dem Online-Spieler eine personalisierte Webseite präsentiert wird, die alle von ihm vorgenommenen Einstellungen berücksichtigt, kann dies für ihn komfortabel sein. Allerdings besteht bei dem Einsatz von solchen persistenten Cookies eine datenschutzrechtliche Problematik, wenn sich mit Hilfe der Cookies (etwa durch Einbindung einer eindeutigen ID) ein Personenbezug herstellen lässt. Ist der Nutzer bereits bei dem Spiele-Betreiber bestimmbar, unabhängig davon, ob dies durch Registrierung erfolgt oder durch entsprechende Informationen per Cookie, so sind auch die zusätzlich anfallenden zuordenbaren Daten personenbezogen. Grundsätzlich sind auch für Cookies die Datenschutzgesetze anwendbar, wenn sie eine Identifizierung des Spielers ermöglichen. Nach § 13 Abs. 1 Satz 2 TMG bestehen für den Anbieter besondere Hinweispflichten auf den Einsatz dieser Technik. Selbst wenn nur eine Nummer in einem längerfristig gespeicherten Cookie hinterlegt ist, so ermöglicht diese doch die Widererkennung eines Spielers. Wird diese genutzt, um z. B. ein Spielerprofil anzulegen, so ist § 15 Abs. 3 TMG zu beachten und der Spieler auf sein Widerspruchsrecht hinzuweisen.

Weitreichende Änderungen in diesem Bereich können sich durch die EU-Richtlinie 2009/136/EG vom 25.11.2009 ergeben. Unter anderem ist dieser zu entnehmen, dass das Setzen von (permanenten) Cookies auf einer Einwilligung des Betroffenen beruhen soll. Insbesondere für Betreiber von Browser-Spielen kann dieses relevant sein. Entsprechende Anpassungen im nationalen Recht müssen bis zum 25.05.2011 erfolgt sein.

8.3 Exkurs

8.3.1 Datenschutz auch für Avatare?

Grundsätzlich ist das Datenschutzrecht als Ausfluss des allgemeinen Persönlichkeitsrechts nur auf (natürliche) Personen anwendbar. Ein Avatar ist jedoch eine von einem Spieler

künstlich geschaffene Person in der virtuellen Welt.[104] Dem Spieler „hinter“ dem Avatar wird nicht nur das Recht an diesem selbst zugesprochen; vielmehr stellen Eingriffe in die Rechte am Avatar und Eingriffe in „dessen“ Rechte Verletzungen eines Immaterialrechtsgutes dar. Zum einen wird angenommen, dass das Recht am Avatar als sonstiges Recht im Sinne des § 823 Abs. 1 BGB geschützt ist.[105] Zum anderen könnte der Avatar über eine besonders geschützte Rechtsposition verfügen, weswegen auch Verstöße gegen das Datenschutzrecht hinsichtlich des Avatars rechtliche Relevanz entfalten können.

So ist davon auszugehen, dass Avatare Ersatz des bürgerlichen Namens, nämlich ein Pseudonym für den Spieler, sein kann und zwar dann, wenn mit dem Pseudonym ausschließlich eine Person in Verbindung zu bringen ist.[106] Das Pseudonym ist Ausdruck des spielerischen und entsprechend gesellschaftlichen Wirkens des Namensträgers.

Besondere Rechte für die Avatare werden deshalb beispielsweise über das Recht am eigenen Bild als Ausfluss des allgemeinen Persönlichkeitsrechts hergeleitet und zwar dann, wenn der Avatar die reale Person widerspiegelt.[107] Datenschutzrechtlich ist auch der Schutz des Namens des Avatars von Bedeutung, wenn diesem Verkehrsgeltung zukommt. Dies setzt voraus, dass der Spieler in den entsprechenden Verkehrskreisen unter dem Pseudonym bekannt ist und das Pseudonym den bürgerlichen Namen so verdrängt hat, dass es dessen Funktion übernommen hat.[108] Darüber hinaus wird auch der virtuellen Identität an sich in Gestalt des Avatars zumindest teilweise ein eigener Rechtscharakter zugeschrieben.[109] Hieraus folgt, dass auch für die Nutzung von Spielangeboten mit Avataren die datenschutzrechtlichen Bestimmungen greifen können. Dies ist abhängig von der Gestaltung des Avatarnamen und der Bestimmbarkeit der hinter dem Avatar stehenden Person.

8.3.2 Datenschutz und Prävention für Online-Spieler

Zum Schutz der Spieler von Online-Spielen werden die Betreiber in Verbraucherschutzforen, Jugendschutzforen u. ä. immer wieder aufgerufen, Sicherheitslücken in den Online-Spielen zu beheben und Schutzmaßnahmen zu ergreifen. Das „Forum des droits sur l’internet“ forderte im Jahre 2008 in einem Grundsatzpapier die Überwachung und Regulierung von Computerspielen im Internet.[110] In diesem Grundsatzpapier fordert dieses Forum Rahmenregelungen für Online-Spiele zum Schutz der Spieler, Eltern und Spielentwickler. Es wird unter

[104] Habel, in: MMR 2008, S. 71 (72).

[105] Koch, Die rechtliche Bewertung virtueller Gegenstände auf Online-Plattformen, Abs. 48 http://www.jurpc.de/aufsatz/20060057.htm.

[106] Koos, in: GRUR 2004, S. 808 (810).

[107] Geis / Geis, in: CR 2007, S. 721 (725).

[108] Bayreuther, in: Rebmann / Säcker / Rixecker (Hrsg.), MüKo, 5. Auflage 2006, Band 1, § 12, Rn. 25; Geis / Geis, in: CR 2007, S. 721 (724).

[109] Krasemann, in: DUD 2008, S. 194 (195).

[110] Dazu ausführlich: Buron, in: MMR 2008, S. XVIII.

anderem zum Schutz der Spieler vorgeschlagen, Spielfiguren mit Ermüdungserscheinungen zu versehen, um damit zu exzessives Spielen zu unterbinden. Weiterhin sollen die Spieler Urheberrechte an der von ihnen geschaffenen Spielfigur (Avatar) erhalten. Im Bereich der Werbung wird der Vorschlag unterbreitet, In-Game-Advertising nur entsprechend den für die Spiele geltenden Altersstufen zuzulassen bzw. bei Nutzung der Spiele durch Kinder und Jugendliche Werbung ganz zu verbieten. Als eine weitere Möglichkeit zum Schutz der Spieler wird vorgeschlagen, in die Software einen Hinweis auf die bereits verspielte Zeit einzubinden oder eine Mitteilung zu übermitteln, eine Pause einzulegen.

Diese vorgeschlagenen Präventionsmaßnahmen beinhalten auch datenschutzrechtliche Fragen, die einer weitergehenden Analyse bedürfen. Datenschutzrechtliche Fragen bestehen insbesondere darin, dass für eine Suchtprävention im Zweifel Gesundheitsdaten erforderlich sind, die einem strengeren Schutz als sonstige personenbezogene Daten unterliegen, § 3 Abs. 9 BDSG. Derartige Maßnahmen bedürfen dann auch einer Verhaltensanalyse der Spieler, die datenschutzkonform gestaltet werden muss. Insoweit besteht in diesem Rahmen ein weitergehender Forschungsbedarf.[111]

[111] Siehe dazu Kapitel 13.

9 Leitfaden für Hersteller, Publisher und Betreiber von Online-Spielen

9.1 Einleitung

Dieser Leitfaden kann Herstellern, Publishern und Betreibern von Online-Spielen als Hilfestellung dienen, um Online-Spiele datenschutzgerecht zu entwickeln und anzubieten. Zwar kann der Leitfaden nicht im Detail auf jede denkbare Datenverarbeitung in einem Online-Spiel eingehen. Um dennoch den vielfältigen Varianten von Online-Spielen vom Browsergame, über Handy- und Konsolenspiele bis zum komplexen Online-Rollenspiel gerecht zu werden, ist dieser Leitfaden modular aufgebaut. Nach dem Baukastensystem können Entwickler und Betreiber die Module heraussuchen, die in ihrem Produkt eine Rolle spielen. Eine Vollständigkeit der Abhandlung kann aufgrund der Vielzahl möglicher Konstellationen in der globalisierten und dynamischen Welt der Online-Spiele nicht erreicht werden. Vielmehr sollen die Angaben zu Restriktionen und insbesondere die Lösungsvorschläge Denkanstöße bieten und zu einer eigenen Erarbeitung von passgenauen Lösungen motivieren.

Ist in diesem Leitfaden von „Daten“ die Rede, so sind in der Regel hierunter personenbezogene Daten zu verstehen. Nur für diese gelten die hier aufgestellten Vorschriften zum Datenschutz. Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG). Soweit das TKG einschlägig ist, können auch Daten von juristischen Personen in diesem Sinne relevant sein. Unter dem Begriff der personenbezogenen Daten können alle Informationen fallen, die einen Bezug zu einer Person haben. Im Rahmen von Online-Spielen sind dieses neben Bestandsdaten wie Name, Adresse etc. u. a. auch Daten, die Rückschlüsse auf das Verhalten des Spielers erlauben. Selbst die reine Wiedererkennung eines Spielers kann datenschutzrechtliche Relevanz haben, auch wenn die Person nicht unmittelbar über Name oder Adresse identifiziert ist.

Die hier vorgestellten Datenschutzvorgaben beziehen sich insbesondere auf die Daten verarbeitende Stelle, also die Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG). Dies sind in der Regel die Betreiber des Spiels, was auch unterstützende Dienstleister mit einbeziehen kann. Doch auch für die Entwicklung von Online-Spielen sind die Informationen in diesem Leitfaden interessant, um schon beim Design und der Implementierung des Spiels die rechtlichen Vorgaben einzuhalten bzw. die Umsetzung der Rechte zu vereinfachen.

Der Schwerpunkt der Darstellung liegt auf dem deutschen Datenschutzrecht. Dieses ist in der Regel einschlägig, wenn sich ein Online-Spiel (auch) an deutsche Spieler richtet. Grundsätzlich gilt für diesen Bereich das Herkunftslandprinzip nach § 3 TMG. Sofern der Spiele-Betreiber zumindest eine Niederlassung in Deutschland hat, sind die hier großenteils rele-

vanten Normen des Telemediengesetzes anwendbar. Befinden sich Niederlassungen nicht in Deutschland, sondern im europäischen EU-Ausland, so sind die dortigen Normen heranzuziehen, die im Bereich des Datenschutzes in großen Teilen vergleichbar mit denen in Deutschland sind, da sie auf die selben Datenschutzrichtlinien der EU zurückgehen. Auch bleibt das für den Schutz personenbezogener Daten geltende Recht unberührt vom Herkunftslandprinzip (vgl. § 3 Abs. 3 Nr. 4 TMG).

9.2 Datenschutzrelevante Funktionen in Online-Spielen

9.2.1 Generelle Vorkehrungen

a) Funktionalitätsbeschreibung

Wer Online-Spiele betreibt, betreibt in der Regel auch automatisierte Datenverarbeitung. Wer hierbei personenbezogene Daten verarbeitet, hat generelle Vorkehrungen dafür zu treffen, dass die Daten nur gesetzeskonform verarbeitet werden. Dazu gehört insbesondere, dass Dritte keinen unberechtigten Zugriff auf diese Daten erhalten und Spieler ihre Datenschutzrechte durchsetzen können. Bei Online-Spielen ist wie auch bei jedem anderen Online-Angebot zu beachten, dass es sich nach herrschender Meinung in Deutschland schon bei der IP-Adresse des Nutzers um ein personenbezogenes Datum handelt, so dass generell alle Betreiber von Spielen im Internet vom Datenschutzrecht betroffen sind. Jedes Daten verarbeitende Unternehmen sollte außerdem ein Datenschutzmanagementsystem intern etabliert haben, das mehr ist, als die Benennung eines Datenschutzbeauftragten.

b) Relevante Normen

- § 13 Abs. 4 TMG, § 9 BDSG und Anlage zu § 9 Satz 1 BDSG: Technisch-organisatorische Vorkehrungen
- §§ 4d ff., 5, 6 BDSG: Datenschutzbeauftragter
- § 3a BDSG: Datenvermeidung und Datensparsamkeit
- § 13 Abs. 6 TMG: Nutzung anonym oder unter Pseudonym
- §§ 6, 33ff. BDSG, § 13 Abs. 7 TMG: Betroffenenrechte

c) Restriktionen

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist nach Anlage zu § 9 Satz 1 BDSG die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

(Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Eine Maßnahme zur Zugangskontrolle, Zugriffskontrolle und Weitergabekontrolle ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Erforderlich sind diese Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Daten, die für unterschiedliche Zwecke oder Spiele erhoben wurden (z. B. zu Abrechnungszwecken und für Marketing), sind getrennt voneinander zu verarbeiten. Der Spieler muss hierüber informiert sein und die Nutzung des Spiels jederzeit beenden können.

Erhobene personenbezogene Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung müssen nach Wegfall der Erforderlichkeit gelöscht oder, wenn Aufbewahrungspflichten etwa nach der Abgabenordnung (AO) oder dem Handelsgesetzbuch (HGB) bestehen, gesperrt werden. Sperren ist hierbei das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

Der Nutzer muss das Online-Spiel gegen Kenntnisnahme unberechtigter Dritter geschützt in Anspruch nehmen können, so dass im Rahmen des technisch Möglichen und Zumutbaren eine Verschlüsselung der Online-Verbindung erforderlich sein kann. Die Gewährleistung der Datensicherheit schließt auch ein, dass ein systematischer oder massenhafter Export oder Download von Profildaten aus dem Online-Spiel durch unberechtigte Dritte etwa automatisiert durch sog. Crawler verhindert werden muss.

Unternehmen mit mehr als neun Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, haben einen Datenschutzbeauftragten zu

bestellen. Die mit der Datenverarbeitung beschäftigten Personen sind auf das Datengeheimnis zu verpflichten.

Die Spieler haben die Rechte auf Auskunft, Berichtigung und Löschung / Sperrung. Die Umsetzung dieser Rechte ist durch den Betreiber (ggf. Hersteller) so zu gewährleisten, dass sie jeweils zeitnah realisiert werden können. Dies bedeutet insbesondere, dass die Datenbanken entsprechend organisiert werden und Zugriffs- und Abfragemöglichkeiten bereitgehalten werden. Dies bezieht sich auch auf Daten, die unter einem Pseudonym organisiert sind und bei denen der Betreiber Zugriff auf die Zuordnung des Pseudonyms zu einer Person hat.

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten bzw. bei der Gestaltung des Online-Spiels ist die Zielsetzung zu berücksichtigen, so wenige personenbezogene Daten wie möglich zu verarbeiten. Soweit möglich und zumutbar, sind die Daten zu anonymisieren bzw. pseudonymisieren. Insbesondere hat der Betreiber die Nutzung des Spiels und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Hierüber ist der Spieler zu informieren.

d) Mögliche Lösungen

- Folgende Dokumente sollten erstellt werden, um eine interne Kontrolle (Innenrevision) zu ermöglichen und eine externe Kontrolle (durch die zuständige Aufsichtsbehörde) zu erleichtern: Verfahrensdokumentation, Sicherheitsmaßnahmen / Risikoanalyse, Dokumentation von Test und Freigabe.
- Verfahren und Prozesse sind einzurichten und zu dokumentieren, die in Fällen des nie auszuschließenden Notfalls / Datenmissbrauchs / Zwischenfalls greifen (Wer ist für was zuständig? Information der Kunden? Notfall-Team auch außerhalb der Geschäftszeiten?).
- Audits durch externe anerkannte Dienstleister können dazu beitragen, die eigenen Vorkehrungen für den Datenschutz (regelmäßig) zu überprüfen (ggf. auch Zertifizierung des Spiels durch das ULD[112] / EuroPriSe[113]).
- Ein unabhängiger betrieblicher Datenschutzbeauftragter ist zu bestellen. Dieser sollte über ausreichende Ressourcen verfügen und sich über Schulungen oder andere Wege regelmäßig in Datenschutzfragen weiterbilden.
- Personenbezogene Daten sind möglichst zu verschlüsseln, so dass nur Personen, die den Schlüssel kennen, Zugriff auf die Daten haben.
- Ein Berechtigungsmanagement ist einzurichten, das sicherstellt, dass nur die Personen mit den vorher definierten Rechten Zugriff auf für ihre Arbeit notwendige Daten haben.
- Die Mitarbeiter sind auf Verschwiegenheit zu verpflichten, und es sind regelmäßige

[112] https://www.datenschutzzentrum.de/guetesiegel/index.htm.

[113] https://www.european-privacy-seal.eu/.

Schulung durch den Datenschutzbeauftragten durchzuführen. Die Verschwiegenheitsverpflichtung ist schriftlich festzuhalten und zu dokumentieren.

- Personenbezogene und personenbeziehbare Daten sind so früh wie möglich so zu anonymisieren, dass eine Identifikation ausgeschlossen werden kann. Sofern dann kein Personenbezug mehr herstellbar ist, unterfallen die Daten nicht mehr den Datenschutzgesetzen.

e) Weiterführende Literatur

- Leitbild u. a. für eine notwendige Dokumentation: Landesverordnung Schleswig-Holstein über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten: https://www.datenschutzzentrum.de/material/recht/dsvo.pdf.
- Artikel 29-Datenschutzgruppe: Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_de.pdf.

9.2.2 Vertrieb

a) Funktionalitätsbeschreibung

Online-Spiele können sowohl klassisch mittels Datenträgern wie auch online an den Endnutzer vertrieben werden. Zu unterscheiden ist jeweils, ob der Vertrieb direkt durch den Betreiber erfolgt oder durch den Publisher oder einen dritten Händler. Beim Online-Vertrieb können in einigen Fällen zusätzlich Spielsysteme Dritter wie von Microsoft (Xbox Live) oder Apple (App Store) genutzt werden (vgl. Abschnitt 9.2.21).

b) Relevante Normen

- §§ 3a, 28 BDSG
- Anlage zu § 9 Satz 1 BDSG
- § 14 TMG

c) Restriktionen

Die Abfrage von personenbezogenen Daten beim Vertrieb des Online-Spiels ist auf die Daten zu beschränken, die für den Vertrieb erforderlich sind. Darüber hinausgehende Datenerhebungen bedürfen der Einwilligung des Nutzers. Es gilt ein Kopplungsverbot: Die verantwortliche Stelle darf den Abschluss eines Vertrages nicht von einer Einwilligung des Betroffenen in die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels und der Werbung abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Die Daten, die zum Zwecke des Vertriebs erhoben werden, sind von den übrigen Bestands- und Nutzungsdaten für den Spielbetrieb zu trennen. Die Vertriebsdaten

sind zu löschen, wenn der Vertriebsvorgang abgeschlossen und die Aufbewahrung nicht mehr erforderlich ist. Für den Nutzer muss transparent sein, wer jeweils Daten verarbeitende Stelle ist und welche personenbezogenen Daten zu welchen Zwecken erhoben und gespeichert werden. Insbesondere ist beim Online-Vertrieb über Art, Umfang und Zweck der Erhebung aufzuklären (vgl. Abschnitt 9.2.16).

d) Mögliche Lösungen

- Die Datenverarbeitung für den Vertrieb des Spiels und die Registrierung für das Spiel selber sind sowohl intern als auch nach außen hin erkennbar voneinander zu trennen. Hierfür sind unterschiedliche Datenbanken anzulegen. Dabei müssen die grundlegenden Bedingungen für die Registrierung auch schon beim Vertrieb für den Spieler erkennbar sein.
- Für den Käufer / Spieler muss stets erkennbar sein, wer die Daten verarbeitet, die er angibt und welche personenbezogenen Daten sonst noch erhoben werden.
- Werden Daten erhoben, die über die für den Vertrieb des Spiels erforderlichen Daten hinausgehen (z. B. Familienstand, Geräteausstattung, ggf. auch genaues Geburtsdatum), so sind diese Daten deutlich als optional bzw. freiwillig darzustellen.
- Es sollten getrennte Datenbanken für den Vertrieb des Spiels und den Betrieb des Spiels eingerichtet werden.
- Es sind automatisierte Löschroutinen einzurichten, die Vertriebsdaten regelmäßig nach Wegfall der Erforderlichkeit löschen.
- Erfolgt der Vertrieb des Spiels über ein Spielsystem eines Dritten, so muss dieses für den Nutzer klar erkennbar sein, sofern keine Auftragsdatenverarbeitung vorliegt.
- Daten, die durch den Vertrieb des Spiels erlangt wurden, dürfen nur dann für andere Zwecke verwendet werden, wenn der Nutzer hierin eingewilligt hat oder eine Rechtsnorm dieses erlaubt.
- Lizenzbedingungen mit Datenschutzinhalten werden nur dann Vertragsbestandteil, wenn der Nutzer diese beim Kauf des Spiels zur Kenntnis nehmen kann. Sie sind daher beim Vertrieb als Datenträger auf die Verpackung zu drucken oder beim Online-Vertrieb klar vor dem Kauf anzuzeigen. Derartige Lizenzbedingungen ersetzen nicht die ausdrückliche Einwilligung des Nutzers.
- Soweit möglich, sind anonyme Zahlungsmethoden (z. B. Prepaid-Karten) auch schon beim Vertrieb anzubieten.
- Werden IP-Adressen des Käufers oder Interessenten beim Vertrieb des Online-Spiels erfasst, so unterliegen sie den Datenschutzgesetzen. Grundsätzlich dürfen sie in diesem Fall nur so lange gespeichert werden, wie sie für die Erbringung des Dienstes (also des Vertriebs) erforderlich sind. Für die Erstellung von Statistiken / Optimierung des Dienstes dürfen sie grundsätzlich gar nicht aufbewahrt werden, sondern müssen in anonymisierter Form ausgewertet werden. Aus Sicherheitsgründen, etwa zur Identifikation von Hacking-

Angriffen oder Betrugsversuchen, ist eine Speicherfrist von maximal sieben Tagen zulässig. Danach müssen sie gelöscht bzw. anonymisiert werden. Dabei müssen diese Daten getrennt vom normalen System verarbeitet und ausgewertet werden.

e) Weiterführende Literatur

- FAQ des ULD zu IP-Adressen: http://www.datenschutzzentrum.de/ip-adressen/.

9.2.3 Installation und Registrierung

a) Funktionalitätsbeschreibung

Online-Spiele müssen ggf. nach dem Kauf / Download installiert werden. Die Betreiber haben dabei ein Interesse daran, Raubkopien zu erkennen. Hierzu werden oftmals bei der Installation Lizenzdaten an den Betreiber übermittelt. Diese sind dann datenschutzrechtlich relevant, wenn sie einen Rückschluss auf die Person des Spielers erlauben, was in Verbindung mit einer IP-Adresse, Cookies, einer Registrierung oder einer Supportanfrage der Fall sein kann. Für das Spielen ist meist eine Registrierung bzw. Anmeldung des Spielers erforderlich, um ihn insbesondere bei späteren Spielen wiederzuerkennen, um Jugendschutzbestimmungen einzuhalten oder um ihm weitergehende Informationen zukommen zu lassen.

b) Relevante Normen

- §§ 11 ff. TMG
- §§ 3a, 28 BDSG

c) Restriktionen

Bei der Registrierung bzw. Anmeldung dürfen nur diejenigen Daten verarbeitet werden, die für den Spielbetrieb erforderlich sind. Darüber hinausgehende abgefragte Daten müssen als solche kenntlich gemacht werden. Verarbeitungszwecke etc. müssen mittels einer Datenschutzerklärung kenntlich gemacht werden (siehe auch dort).

Es muss stets transparent sein, wann welche Daten an wen zu welchem Zweck übermittelt werden.

d) Mögliche Lösungen

- Nur unbedingt erforderlichen Daten (z. B. Nutzername und Passwort) sind beim Spieler abzufragen.
- Daten bei der Anmeldung / Registrierung, die optional sind, sind zu kennzeichnen.
- Die Datenverarbeitung ist so weit wie möglich auf anonyme bzw. pseudonyme Daten zu beschränken. Der Spieler sollte sich somit möglichst nur unter Pseudonym registrieren können. Die E-Mail-Adresse ist in der Regel kein geeignetes Pseudonym, da sie häufig Namensbestandteile enthält, die einen Personenbezug ermöglichen.
- Es darf keine Übermittlung von Daten im Hintergrund ohne Autorisierung durch den Spieler erfolgen.

- Lizenz- und Nutzungsdaten des Spielers sind voneinander getrennt zu verarbeiten.
- Support-Anfragen sind getrennt von den Lizenzdaten und den Nutzungsdaten zu verarbeiten.
- Auf die Speicherung von IP-Adressen ist möglichst zu verzichten bzw. die IP-Adressen müssen so früh wie möglich anonymisiert werden.
- Eine Datenschutzerklärung ist einzurichten, die vor der Registrierung angezeigt / abrufbar ist.
- Bei Verwendung von Cookies muss ein Hinweis hierauf nach § 13 Abs. 1 Satz 2 TMG (vgl. Abschnitt 9.2.16) erfolgen.
- Es ist eine Möglichkeit für den Nutzer einzurichten, über die bei der Registrierung angegebenen Daten Auskunft zu erhalten, sie zu berichtigen und zu löschen, sofern nicht Vertrags- oder Aufbewahrungspflichten eine weitergehende Speicherung verlangen. Ist eine Löschung aus rechtlichen Gründen nicht möglich, so sind die Daten auszusondern und zu sperren.

9.2.4 Betrieb und Überprüfung

a) Funktionalitätsbeschreibung

Während des Online-Spielens werden Daten vom Spieler zum Betreiber übersendet, um den ordnungsgemäßen Betrieb des Online-Spiels sicherzustellen und etwaige technische Manipulationen auszuschließen bzw. aufzudecken.

b) Relevante Normen

- §§ 13, 15 TMG
- §§ 3a, 4a, 28, 31 BDSG

c) Restriktionen

Die Erhebung und Verwendung von personenbezogenen Daten im Rahmen des Betriebs eines Online-Spiels (z. B. der IP-Adresse) ist soweit zulässig, wie es für die Inanspruchnahme und die Abrechnung des Spiels notwendig ist. Hierüber ist der Nutzer zu Beginn der Nutzung in der Datenschutzerklärung nach § 13 Abs. 1 TMG zu informieren. Eine darüber hinausgehende Datenverarbeitung bedarf in der Regel der Einwilligung des Spielers. Dabei muss er vor der Erklärung der Einwilligung umfassend über die mögliche Datenverarbeitung und Weitergabe von Daten aufgeklärt werden. Der Anwendungsbereich von Tools, die Informationen über einen PC sammeln (Scanner / Anti-Cheat-Tools etc.), ist auf das Notwendige zu reduzieren. Dabei sind Abgleiche, ob eigene Dateien des Spiels manipuliert wurden (insbesondere über Hashwerte) unproblematisch. Datenschutzrechtlich relevant sind jedoch Rückmeldungen über installierte Software und insbesondere Inhalte von spielfremden Dateien.

d) Mögliche Lösungen

- Die Datenschutzerklärung ist schon bei der Installation / Registrierung / ersten Inbetriebnahme des Online-Spiels dem Spieler anzuzeigen. Hierin müssen Art, Umfang und Zweck der Datenverarbeitung genannt werden. Auch ist auf Datenverarbeitung außerhalb der EU / des EWR besonders hinzuweisen (vgl. Abschnitt 9.2.16).
- Werden IP-Adressen des Spielers beim Spiel erfasst, so unterliegen sie den Datenschutzgesetzen (insbesondere handelt es sich um Nutzungsdaten i. S. d. § 15 TMG). Grundsätzlich dürfen sie in diesem Fall nur so lange gespeichert werden, wie sie für die Erbringung des Dienstes erforderlich sind. Für die Erstellung von Statistiken oder zur Optimierung des Dienstes müssen sie anonymisiert werden. Aus Sicherheitsgründen, etwa zum Abfangen von Hacking-Angriffen und Manipulationen, ist eine Speicherdauer von maximal sieben Tagen zulässig, wobei darauf zu achten ist, dass diese Daten getrennt von dem restlichen Produktivsystem gespeichert und analysiert werden, um eine „versehentliche“ Zweckänderung zu vermeiden. Danach müssen sie gelöscht bzw. anonymisiert werden. Wurden die Daten zu Abrechnungszwecken erhoben, so müssen sie spätestens sechs Monate nach Rechnungsstellung gelöscht werden.
- Zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Spiels dürfen mit Einwilligung des Nutzers Spielerprofile angelegt werden. Hierbei müssen Pseudonyme verwendet werden. Dem Spieler muss in diesem Zusammenhang ein Widerspruchsrecht eingeräumt und er muss hierüber unterrichtet werden (vgl. § 15 Abs. 3 TMG).
- Bevor Überwachungstools installiert und in Betrieb genommen werden, die personenbeziehbare Daten auf dem Rechner des Spielers erfassen und an den Betreiber weiterleiten, muss der Nutzer hierin einwilligen. Zuvor muss ihm die genaue Funktion des Tools dargestellt werden. Insbesondere muss er darüber informiert werden, welche Daten bzw. Dateien vom Scanvorgang betroffen sind und was an den Betreiber übermittelt wird. Die Einwilligung muss freiwillig sein, so dass ein Spielen auch ohne Einsatz dieser Tools möglich ist. Ist dieses aufgrund der Besonderheiten des Spiels nicht umsetzbar, muss er hierüber schon vor dem Kauf / vor der Registrierung ausdrücklich hingewiesen werden.
- Der Nutzer muss die Möglichkeit haben, den Scanner abzuschalten bzw. zu deaktivieren.
- Das Scanning mit Übermittlung von personenbeziehbaren Daten an den Betreiber muss auf das absolut Notwendige reduziert werden. Werden etwa Screenshots erfasst und übermittelt, dürfen diese nur das Spielfenster betreffen. Können diese Screenshots weitergehende personenbezogene Daten enthalten (z. B. Gesundheitsdaten bei bestimmten Casual-Games oder Chat-Inhalten), ist ganz auf solche Screenshots zu verzichten. Insbesondere ist auf die Erfassung von Dateien zu verzichten, die personenbezogene Daten enthalten können (z. B. Word-Dateien, Cookies, Kalender, Kontaktlisten etc.). Der Spieler muss über den genauen Umfang der Weiterleitung von Daten seines Rechners informiert werden.
- So weit wie möglich ist auf eine Weiterleitung von Daten auf dem Rechner des Spielers

an den Betreiber des Spiels ganz zu verzichten. Kann hierauf nicht verzichtet werden, so sind personenbezogene Daten zu anonymisieren (z. B. bei IP-Adressen durch Löschung der letzten beiden Oktette).

- Muss das Tool, das den Rechner des Spielers analysiert, aktualisiert werden, so ist der Nutzer vor dem Einspielen des Updates zu informieren. Dies beinhaltet auch die Information darüber, welche Änderungen durch das Update vorgenommen werden. Der Spieler muss dieses unterbinden können.
- Erfolgt eine Sperrung des Zugangs des Nutzers aufgrund der Ergebnisse der Überwachung, so ist der Spieler hierüber zu informieren, und es ist ihm eine Möglichkeit zur Stellungnahme einzuräumen.

9.2.5 Bezahlsystem

a) Funktionalitätsbeschreibung

Über den Vertrieb des Spiels (siehe Abschnitt 9.2.2) hinausgehend können von Publishern bzw. Betreibern von Online-Spielen regelmäßige Gebühren für das Spielen eines Online-Spiels oder eines Spiel-Systems verlangt werden. Dies kann auch die Bezahlung von erweiterter Funktionalität oder besonderen virtuellen Gegenständen (Items) umfassen.

b) Relevante Normen

- §§ 13 Abs. 6, 14, 15 TMG
- § 11 BDSG

c) Restriktionen

Der Betreiber des Spiels hat dessen Nutzung und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Hierüber ist der Spieler zu informieren. Abrechnungsdaten dürfen zweckgebunden nur für die Abrechnung des Spiels genutzt werden. Sie dürfen höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden. Eine Verlängerung dieser Frist ist in der Regel nur für die Fälle möglich, in denen Einwendungen gegen die Entgeltforderung erhoben werden.

d) Mögliche Lösungen

- Prepaid-Karten sollten eingesetzt werden, so dass eine anonyme Zahlung durch den Spieler möglich ist. Da dieses inzwischen technisch möglich und in der Regel zumutbar ist, ist dieses sogar für viele Publisher / Betreiber verpflichtend.
- Abrechnungsdaten sind getrennt von anderen Nutzungsdaten aufzubewahren bzw. zu verarbeiten.
- Ist eine vollständige Löschung der Abrechnungsdaten nach Ablauf der Frist aufgrund bestehender Aufbewahrungspflichten nicht möglich, so sind die Daten zu sperren. Hierbei muss sichergestellt sein, dass nur für Zwecke der Aufbewahrungspflicht auf die Daten

zugegriffen werden kann. Die Daten müssen ausgesondert oder zumindest durch ein Flag als gesperrt gekennzeichnet werden. Die Mitarbeiter sind über den besonderen Umgang mit gesperrten Daten zu informieren. Die Sperrung ist in ein Berechtigungskonzept zu integrieren, und soweit möglich sind die Abrechnungsdaten zum Schutz vor unberechtigter Kenntnisnahme zu verschlüsseln.

- Werden Zahlungsinformationen als Bestandsdaten i. S. d. § 14 TMG erfasst (z. B. Kreditkartendaten), so ist auf eine Verschlüsselung der Übertragung zu achten (z. B. SSL-Verschlüsselung). Die Daten sind möglichst verschlüsselt aufzubewahren und dürfen außerhalb eines etwaigen Auftragsdatenverarbeitungsverhältnisses nicht weitergegeben werden. Sie sind umgehend zu löschen, wenn sie nicht mehr erforderlich sind (z. B. wenn das Spiel-Abonnement ausgelaufen ist und keine Aufbewahrungspflicht besteht).
- Wird mit der Abrechnung durch den Betreiber (Auftraggeber) ein Auftragnehmer beauftragt, so ist zwischen den beiden Parteien ein Vertrag notwendig, der den Vorgaben des § 11 BDSG entspricht. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, was er auch zu dokumentieren hat. Der Betreiber bleibt jedoch verantwortliche Stelle, wenn der Spieler seine Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung geltend macht.
- Eine Auftragsdatenverarbeitung im Rahmen der Erbringung des Online-Spiels ist in der Regel ausgeschlossen, wenn der Auftragnehmer die Daten außerhalb der EU verarbeitet. Im Rahmen einer Datenverarbeitung nach BDSG kann unter besonderen Umständen eine Auftragsdatenverarbeitung dennoch möglich sein (siehe Abschnitt 7.1.3.2.3). Liegt keine Auftragsdatenverarbeitung vor, so ist für eine Übermittlung der Daten an eine Stelle außerhalb der EU die ausdrückliche Einwilligung des Spielers erforderlich. Hierbei ist zu beachten, dass es kein „Konzernprivileg“ gibt. Das bedeutet, dass selbst wenn eine der beiden Parteien ein selbstständiges Tochterunternehmen des anderen ist, eine Übermittlung nur unter den o. g. Bedingungen erlaubt ist.

9.2.6 Kündigung / Spielbeendigung

a) Funktionalitätsbeschreibung

Je nach Geschäftsmodell des Betreibers kann eine Kündigung des Betreibers oder Spielers notwendig sein, um den Online-Spiel-Vertrag zu beenden. Bei Spielen, die nur eine Registrierung erfordern, kann eine Funktion zur Löschung des Accounts vom Betreiber angeboten werden oder einfach das weitere Spielen durch den Spieler unterbleiben.

b) Relevante Normen

- § 14 Abs. 1 TMG
- § 6 Abs. 1 BDSG

c) Restriktionen

Mit der Kündigung oder Löschung des Accounts oder auch bei längerem Unterbleiben des Spiels entfällt mangels Erforderlichkeit der Rechtsgrund für die Speicherung der Bestands- und Nutzungsdaten des Spielers. Daher müssen die Daten ab diesem Zeitpunkt gelöscht bzw. bei Aufbewahrungspflichten gesperrt werden; sie dürfen ohne Einwilligung des Nutzers nicht auf Vorrat gespeichert bleiben.

d) Mögliche Lösungen

- Der Spieler sollte insbesondere dann, wenn der Spiel-Vertrag online geschlossen wurde, die Möglichkeit haben, diesen auch online wieder zu kündigen.
- Der Spieler muss vom Betreiber darüber informiert werden, wie (auf welchem Wege und in welcher Form) er den Vertrag kündigen kann bzw. einen Account löschen kann. Hierzu sollte ein entsprechender Button oder ein Formular an der Stelle angeboten werden, an der auch der Vertrag geschlossen wurde bzw. die Anmeldung erfolgte.
- Nach der Kündigung müssen Bestands- und Nutzungsdaten gelöscht werden, sofern sie nicht noch zur Abwicklung des Vertrages notwendig sind (etwa zur Eintreibung von offenen Posten).
- Ein gesondertes Vorhalten der Daten für eventuell spätere Anfragen durch Strafverfolgungsbehörden ist in der Regel nicht erforderlich und damit auch nicht zulässig.
- Bei kostenlosen Spielen muss eine Möglichkeit bestehen, den Account vollständig zu löschen.
- Es reicht in der Regel nicht aus, die Daten nur in der Datenbank als „gelöscht“ zu markieren, sondern die Daten müssen rückstandsfrei entfernt werden.
- Sofern Aufbewahrungspflichten (z. B. im Rahmen des Handelsrechts / der Abgabenordnung) bestehen, tritt an Stelle der Löschung die Verpflichtung zur Sperrung der Daten.
- Sollen Account- bzw. Vertragsdaten über die Aufbewahrungspflichten und die Vertragslaufzeit hinaus gespeichert werden (etwa um dem Spieler eine vereinfachte Rückkehr zu ermöglichen bzw. ihn über neue Angebote zu informieren), so muss der Spieler hierin und auch in die weitere Verwendung der Daten ausdrücklich einwilligen.
- Eine Löschungspflicht kann auch bestehen, wenn ein (kostenloses) Spiel sehr lange nicht benutzt wurde und davon auszugehen ist, dass der Spieler kein Interesse mehr an seinen Account hat. Die Frist hierfür kann großzügig bemessen werden und richtet sich danach, wann nach vernünftigem Ermessen nicht mehr mit der Rückkehr des Spielers zu rechnen ist.
- Der Spieler muss eine Kontaktmöglichkeit zum Betreiber des Spiels haben, um auch beim Vergessen von Zugangsdaten eine Löschung seiner personenbezogenen Daten zu erreichen. Ggf. muss er sich über andere Legitimationswege hierfür identifizieren. Diese Möglichkeit muss ihm eingeräumt werden.
- Das Recht auf Löschung kann nicht durch Rechtsgeschäft ausgeschlossen oder be-

schränkt werden. Selbst wenn der Spieler in eine weitergehende Speicherung einwilligt, so hat er jederzeit das Recht, diese Einwilligung zu widerrufen.

9.2.7 Spieler-zu-Spieler-Erkennbarkeit

a) Funktionalitätsbeschreibung

Spiele können die Möglichkeit anbieten, innerhalb des Online-Spiels nach anderen Spielern zu suchen und diese im Spiel wiederzuerkennen (z. B. über Freundeslisten bzw. „Buddy-Lists“).

b) Relevante Normen

- § 13 Abs. 6 TMG
- §§ 4 Abs. 1, 4a BDSG

c) Restriktionen

Der Betreiber des Spiels muss im Rahmen des technisch Möglichen und Zumutbaren eine anonyme oder pseudonyme Nutzung des Spiels ermöglichen. Dies beinhaltet auch, dass die Anonymität bzw. Pseudonymität gegenüber den anderen Spielern gewahrt bleibt. Stellt der Betreiber anderen Spielern die Spieldaten eines Nutzers zur Verfügung, so handelt es sich um eine Weitergabe von personenbezogenen Daten an Dritte. Hierfür benötigt er die Einwilligung des Spielers. Der Spieler muss dazu vor Spielbeginn darüber informiert werden, welche Daten von ihm anderen Spielern zur Verfügung gestellt werden, und muss selbst entscheiden können, ob er dieses wünscht.

Zu beachten ist, dass auch pseudonyme Daten in der Regel den Datenschutzgesetzen unterfallen und deren Weitergabe restriktiv gehandhabt wird.

d) Mögliche Lösungen

- Dem Spieler wird ermöglicht, innerhalb des Spiels unter Pseudonym aufzutreten. Dabei wird er bei der Wahl seines Spielernamens / Accountnamens darauf hingewiesen, dass er aus Datenschutzgründen ein Pseudonym verwenden sollte, das keinen Rückschluss auf seine Person ermöglicht.
- Die Voreinstellung im Spiel sollte so gewählt werden, dass die Weitergabe von Spieldaten an andere Spieler so restriktiv wie möglich gehandhabt wird.
- Der Spieler muss darüber informiert werden, welche Daten an andere Spieler übertragen werden bzw. für diese einsehbar sind.
- Bei entsprechend ausgelegten Spielen sollte der Spieler auch differenzieren können zwischen den Daten, die er an alle Mitspieler, die er nur an seine „Freunde“ (sofern eine Freundesliste bzw. Buddy-List existiert) und welche gar nicht weitergegeben werden dürfen.
- Der Spieler sollte auch im Nachhinein eine Möglichkeit zur Abfrage haben, welche Daten an wen weitergegeben wurden.

9.2.8 Reputationssystem / Beschwerdemanagement

a) Funktionalitätsbeschreibung

Das Spiel ermöglicht eine Bewertung der Spieler untereinander. Hiermit kann beispielsweise gegenüber den Mitspielern und dem Betreiber signalisiert werden, ob sich jemand nicht an die Spielregeln hält (z. B. Abbruch einer Partie kurz vor Ende bei drohendem Verlust) oder anderweitig auffällt (Äußerung von Beleidigungen etc.). Aber auch Mitspieler können ggf. bei entsprechender Einbindung Rückschlüsse darauf ziehen, welche Mitspieler für sie geeignet sind. Dabei können sie auch andere Spieler vor bestimmten Personen warnen oder auch Spieler empfehlen.

Mittels eines Formulars kann auch dem Spieler die Möglichkeit eingeräumt werden, sich direkt beim Betreiber über einen Mitspieler zu beschweren.

b) Relevante Normen

- §§ 28 ff. BDSG

c) Restriktionen

Die Einrichtung einer Beschwerdefunktion gegenüber dem Betreiber ist nicht nur in der Regel zulässig, sondern ggf. aus Jugendschutzgründen sogar wünschenswert bzw. notwendig. Das dabei angewendete Verfahren muss jedoch transparent sein. Problematisch ist die Einrichtung von „schwarzen Listen“ von auffällig gewordenen Spielern. Der Spieler muss darüber informiert werden, wenn er hierauf eingetragen wird bzw. anderweitige Restriktionen aufgrund von Beschwerden vorgenommen werden. Dabei muss ihm die Möglichkeit zu einer Stellungnahme geboten werden, die auch die Möglichkeit offen lässt, dass der Betreiber den Spieler wieder von der Liste nimmt. Die Einträge auf der Liste sind zu befristen und regelmäßig auf ihre Erforderlichkeit hin zu untersuchen.

Auch ein Reputationssystem, das für andere Spieler einsehbar ist, muss transparent gestaltet werden und sollte nur auf relevanten Kriterien beruhen. Schon vor Spielbeginn muss der Spieler darüber informiert werden, dass eine solche Funktionalität vorhanden ist. Einem bewerteten Spieler muss die Möglichkeit zur Stellungnahme gegeben werden. Wünscht ein Spieler die Löschung seines Accounts, so sind auch die ihn betreffenden Eintragungen im Reputationssystem zu entfernen.

d) Mögliche Lösungen

- Das Beschwerdeverfahren muss transparent gestaltet werden. Über eingegangene Beschwerden sollte der Betroffene informiert und eine Möglichkeit zur Stellungnahme gegeben werden.
- So weit wie möglich ist auf „schwarze Listen“ zu verzichten. Kann hierauf nicht verzichtet werden, so darf ein Eintrag nur nach transparenten Kriterien erfolgen. Einträge auf der Liste sind zu löschen, wenn sie zum Schutz der Spieler nicht weiter erforderlich sind. Die betroffene Person ist über den Eintrag zu informieren.
- Reputationssysteme sind transparent zu gestalten; alle Spieler müssen informiert wer-

den. Wird ein Spieler bewertet, so ist er hierüber zu informieren, und es muss ihm eine Möglichkeit zur Stellungnahme eröffnet werden.

- Bewertungen sollten einem automatischen Alterungsprozess unterliegen, so dass nach einer angemessenen Zeit alte und weniger relevant gewordene Bewertungen gelöscht werden. Damit wird ein Nutzer nicht noch über Jahre oder Jahrzehnte mit etwaigen „Jugendsünden“ konfrontiert, die keine Relevanz mehr besitzen.
- Kündigt ein Spieler bzw. löscht er seinen Account, so müssen auch die Bewertungen in der Regel im gesamten System umgehend gelöscht werden.
- Bewertungen sollten nur für die Spieler einsehbar sein, für die diese relevant sind.
- Bewertungen sollten sich möglichst nur auf die pseudonymen Spielernamen beziehen.
- Ein Austausch von Bewertungen / schwarzen Listen etc. mit anderen externen Spiele-Betreibern ist in der Regel nicht zulässig. Eine Ausnahme kann bestehen, wenn ein rechtskräftiges Urteil gegen einen Spieler etwa wegen Betrugs vorliegt.

9.2.9 Highscoreliste

a) Funktionalitätsbeschreibung

Highscorelisten dienen der einfachen Präsentation von Spielergebnissen gegenüber anderen Spielern bzw. der Online-Welt. Diese können innerhalb eines Spiels vorgehalten werden oder auch von extern einsehbar sein.

b) Relevante Normen

- § 13 Abs. 6 TMG
- § 15 TMG
- § 4a BDSG

c) Restriktionen

Das Verfahren für die Eintragung auf Highscorelisten ist transparent zu gestalten. Eine Veröffentlichung von Spielerdaten (Pseudonym, erbrachte Leistung, Datum etc.) darf nur nach Einwilligung erfolgen. Diese kann ggf. auch schon bei der Registrierung / Anmeldung zu dem Spiel geschehen. Über Eintragungen auf Highscorelisten ist der Spieler zu informieren.

d) Mögliche Lösungen

- Ein Eintrag auf einer Highscoreliste sollte möglichst manuell vom Spieler freigeschaltet werden. Hierbei sollte er darüber informiert werden, wer diesen Eintrag einsehen kann und was er enthält.
- Der Spieler muss die Möglichkeit haben, für den Eintrag ein Pseudonym zu wählen.
- Kündigt der Spieler bzw. löscht er seinen Account, so sind auch die Einträge auf den Highscorelisten zu entfernen, sofern der Spieler nicht ausdrücklich etwas anderes

wünscht. Willigt der Spieler in eine längere Speicherung ein, so muss er dennoch jederzeit die Möglichkeit haben, die Einträge wieder löschen zu lassen. Hierzu sollte ihm ein Passwort oder eine andere Identifikationsmöglichkeit zur Verfügung gestellt werden.

- Soweit möglich, ist auf zu präzise Datumsangaben in der Highscoreliste zu verzichten. Je nach Spieltyp kann die Angabe der Woche oder des Monats ausreichen. Ggf. kann ganz auf eine Angabe des Zeitpunkts verzichtet werden.
- Besonderer Aufmerksamkeit bedürfen Einträge, die Aussagen über den Gesundheitszustand einer Person treffen (z. B. Gewicht des Spielers, Ausdauer etc.). Für die Veröffentlichung dieser Daten ist eine gesonderte Einwilligung einzuholen.
- Einträge auf Highscorelisten sollten einem automatischen Alterungsprozess unterliegen, so dass nach einer für das Spiel angemessenen Zeit Einträge entweder gelöscht oder anonymisiert werden.

9.2.10 Ligamodus

a) Funktionalitätsbeschreibung

Eine besondere Art der Präsentation von Spielergebnissen ist der Ligamodus. Er zeichnet sich dadurch aus, dass über mehrere Spiele / Partien hinweg Punkte gesammelt werden, aus denen ein Ranking erstellt wird. In der Regel setzen sich die Partien aus Spielen zwischen Teilnehmern der entsprechenden Liga zusammen.

b) Relevante Normen

- §§ 13, 15 TMG
- § 4a BDSG
- § 28 BDSG

c) Restriktionen

Die Datenverarbeitung im Rahmen des Ligamodus ist transparent zu gestalten. Die Mitspieler müssen wissen, welche Daten von wem eingesehen werden können. Im Rahmen des technisch Möglichen und Zumutbaren sind nur pseudonyme Daten darzustellen. Da im Ligamodus die Leistungsmessung zwischen einzelnen Spielern im Vordergrund steht und diese in Verhältnis zu einer Saison gesetzt wird, sind die Löschungsrechte des einzelnen Teilnehmers während der laufenden Saison ggf. eingeschränkt. Dies sollte den Spielern jedoch vorab mitgeteilt werden. Nach Abschluss einer Saison sind die personenbezogenen Daten zu löschen, sofern keine Einwilligung der Spieler in eine weitergehende Speicherung und Präsentation etwa in Form eines Archivs vorliegt.

d) Mögliche Lösungen

- Deutliche Hinweise über die Funktion des Ligamodus, gespeicherte Datenarten, präsentierte Datenarten, Personengruppen mit Zugriffsrechten, Einschränkung der vorzeitigen Löschung der Daten und Aufbewahrungsfristen sollten schon bei Registrierung zu dem

Spiel mitgeteilt werden.

- Die Möglichkeit unter einem Pseudonym zu spielen, das nicht den Rückschluss auf die Identität der dahinter stehenden Person zulässt, ist einzurichten.
- Die Spielergebnisse sind in der Regel nach Abschluss der Saison zu löschen, sofern durch die Spieler keine Einwilligungen für eine weitergehende Verarbeitung gegeben wurden.
- Sollen die Ligaergebnisse längerfristig gespeichert und präsentiert werden, muss hierfür eine Einwilligung durch den Spieler eingeholt werden. Hierbei ist zu beachten, dass diese Einwilligung auch jederzeit widerrufen werden kann, so dass dann diese Daten gelöscht werden müssen.
- Bei hochklassigen Ligen, internationalen Meisterschaften etc. kann das Interesse der Allgemeinheit an der Aufbewahrung der Ligaergebnisse bestehen, so dass daher das Interesse des einzelnen Teilnehmers zurückstehen muss. Ein Löschungsrecht würde in diesem Fall entfallen. Jedoch dürfte zurzeit ein solcher Fall nur selten vorliegen.

9.2.11 Eigenpräsentation des Spielers

a) Funktionalitätsbeschreibung

Einige Spielsysteme unterstützen den Wunsch von Spielern, ihre Spielhistorie und insbesondere ihre Spielleistungen zu präsentieren. Dies kann Informationen über gespielte Spiele, Spielzeiten, erreichte Punktzahlen / Achievements, besiegte Mitspieler etc. beinhalten. Diese Informationen können einem eingeschränkten Mitspielerkreis, allen Nutzern eines Spielsystems oder der ganzen Welt (z. B. über das Internet) präsentiert werden.

b) Relevante Normen

- § 13 Abs. 6 TMG
- § 15 TMG
- § 4a BDSG
- § 28 BDSG

c) Restriktionen

Vor Aktivierung der Leistungspräsentation muss dem Spieler bekannt gegeben werden, welche seiner Spieldaten für welche Personen einsehbar sind und wie die Veröffentlichung eingeschränkt werden kann. Standardeinstellungen sind möglichst restriktiv zu wählen, so dass die Weitergabe von Daten nur nach aktiver Freigabe durch den Spieler erfolgt. Außerdem haben die Betreiber ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

d) Mögliche Lösungen

- Voreinstellung sind so wählen, dass Daten nur nach aktiver Freigabe des Spielers an

andere Spieler oder weitere externe Personen übermittelt werden.

- Eine Beispielseite kann bereitgehalten werden, bei der der Spieler erkennen können, wie seine Spieldaten anderen Personen präsentiert werden.
- Besonderen Hinweis (Warnung) sollten dem Spieler angezeigt werden, wenn ein Profil für die Öffentlichkeit (z. B. Web) freigegeben wird.
- Es ist dem Spieler eine jederzeitige Möglichkeit zu geben, eine Freigabe wieder einzuschränken.
- Insbesondere bei der Präsentation von Spielerdaten im Web sollten nur pseudonyme Daten verwendet und auf allzu konkrete Daten (z. B. genaues Datum / Uhrzeit) verzichtet werden.
- Bei Minderjährigen sollte die öffentlich einsehbare Präsentation von Spielergebnissen im Web oder im Spielsystem deaktiviert werden.

9.2.12 Upload

a) Funktionalitätsbeschreibung

Spiele können die Funktion beinhalten, dass der Spieler eigene Inhalte in das Spielsystem hochlädt, sei es zur Gestaltung der virtuellen Spielumgebung (z. B. mit eigener Musik oder Fotos) oder um sie Mitspielern zur Verfügung zu stellen. Dies können Fotos, Grafiken, Musikstücke oder auch eigene Level- und Spieldesigns sein.

b) Relevante Normen

- §§ 7, 10 TMG
- §§ 4, 35 BDSG
- § 22 KunstUrhG

c) Restriktionen

Datenschutzrechtlich problematisch ist insbesondere der Fall, dass der Spieler personenbezogene Daten (z. B. Fotos) von Dritten in das Spiel integriert und damit anderen Personen zur Verfügung stellt. Damit dürfte in der Regel der Bereich der ausschließlichen Nutzung für persönliche oder familiäre Tätigkeiten i. S. d. § 1 Abs. 2 Nr. 3 BDSG überschritten sein. Der Spieler muss sicherstellen, dass er hierfür die Einwilligung des Dritten hat. Der Spiele-Betreiber ist wiederum je nach Ausgestaltung der Hochlademöglichkeit und des Gefahrenpotentials, dass hierbei Persönlichkeitsrechte Dritter verletzt werden, zur Aufklärung verpflichtet.

Darüber hinaus muss der Betreiber dem Spieler die Möglichkeit bieten, mit dem Hochladen verbundene personenbezogene Daten wieder zu löschen. Auch Dritte, die eine Verletzung z. B. ihres Rechts am eigenen Bild feststellen, müssen eine Kontaktmöglichkeit gegenüber dem Betreiber haben. Vom Betreiber müssen Verfahren bereitgehalten werden, die dann zur Anwendung kommt, wenn sich Dritte über hochgeladene Inhalte beschweren.

d) Mögliche Lösungen

- Dem Hochladen von Inhalten sollte die Erklärung vorangestellt werden, dass die Verwendung von personenbezogenen Daten von Dritten (z. B. von Fotos) nur mit Einwilligung des Betroffenen zulässig sind.
- Der Spieler sollte ausdrücklich – beispielsweise durch Anklicken einer Checkbox – erklären, dass keine Rechte Dritter verletzt werden.
- Der Spieler muss vor dem Hochladen darüber aufgeklärt werden, was mit den hochgeladenen Inhalten passiert, wer hierauf Zugriff hat und welche Möglichkeiten zur Entfernung bestehen.
- Der Spieler sollte jederzeit einen Überblick darüber bekommen können, welche Inhalte von ihm hochgeladen wurden. Dabei muss der Spieler die Möglichkeit haben, diese Inhalte wieder zu löschen.

9.2.13 Chat

a) Funktionalitätsbeschreibung

Die Betreiber können den Spielern die Möglichkeit bieten, in Echtzeit zu kommunizieren. Dies kann mittels Texteingabe, Gesten oder sogar per Audio- oder Videochat (vgl. Abschnitt 9.2.23) geschehen.

b) Relevante Normen

- § 88 TKG
- §§ 11 ff. TMG
- § 202b StGB

c) Restriktionen

Wird in einem Online-Spiel eine Chatmöglichkeit angeboten, so handelt es sich in der Regel um einen Telemediendienst. Richtet sich die Kommunikation an eine beschränkte und klar abgegrenzte Personengruppe, so kann für den Transportweg, auf dem das Telekommunikationsgesetz dann gilt, auch das strenge Fernmeldegeheimnis gelten (siehe Abschnitt 9.2.14).

Chatinhalte dürfen damit für den Fall, dass sie nicht für jedermann einsehbar sind, grundsätzlich nicht unbefugt überwacht oder protokolliert werden. Für eine automatisierte oder manuelle Überwachung der Chatinhalte und für deren Protokollierung zur späteren Analyse ist die Einwilligung aller Teilnehmer erforderlich. Richtet sich der Dienst an Kinder und Jugendliche, so kann es geboten sein, stets eine Moderation durchzuführen. Dies kann z. B. dann der Fall sein, wenn die Gefahr besteht, dass der Chat für (sexuelle) Belästigungen von Erwachsenen gegenüber Kindern genutzt wird. Die Moderation muss jedoch für alle Teilnehmer ersichtlich sein. Ist in einem Chat ein Moderator anwesend, der bei Verstößen gegen die Chatregeln eingreifen kann, so ist dieser als solcher kenntlich zu machen.

d) Mögliche Lösungen

- Es ist Transparenz darüber zu schaffen, wer Einsicht in den Chat hat (z. B. nur von den Teilnehmern explizit zugelassene Personen, der Betreiber oder jeder).
- Soll eine Moderation / Überwachung / Protokollierung durchgeführt werden, so sind die Teilnehmer hierüber zuvor zu informieren und ggf. eine Einwilligung einzuholen.
- Bei Angeboten, die sich an Kinder / Jugendliche richten, kann eine Moderation geboten sein. Diese muss jedoch transparent sein.
- An Stelle der Überwachung / Protokollierung kann den Teilnehmern als milderes Mittel die Möglichkeit eingebaut werden, sich über Chatteilnehmer zu beschweren bzw. Missbrauch zu melden. Hierzu muss zusätzlich ein entsprechendes internes Beschwerdemanagement eingerichtet werden.
- Protokolle sind nach Wegfall der Erforderlichkeit umgehend zu löschen. Die Erforderlichkeit entfällt z. B. im Fall des Zwecks „Schutz der Chatteilnehmer“ dann, wenn mit der Meldung einer Beschwerde nicht mehr gerechnet werden kann (z. B. nach 7 Tagen). Die Löschfristen sind transparent im Rahmen der Datenschutzerklärung mitzuteilen.

e) Weiterführende Literatur

- Dr. Kristina Hopf: Rechtliche Grundlagen des Jugendmedienschutz-Staatsvertrags und die Verantwortlichkeit von Chatbetreibern (ZUM 2008, 207).

9.2.14 Nachrichtenaustausch

a) Funktionalitätsbeschreibung

Während Chatsysteme auf eine Gruppendiskussion ausgelegt sind, bieten zahlreiche Online-Spiele auch die Möglichkeit, dass sich zwei Spieler direkt miteinander austauschen (sog. Personal Message oder auch Private Message (PM)). Hierbei können spielinterne Systeme zum Nachrichtenaustausch und auch Schnittstellen zu einem E-Mail-Dienst angeboten werden.

b) Relevante Normen

- § 88 TKG
- §§ 11 ff TMG
- §§ 100a, 100b, 100g StPO

c) Restriktionen

Bei dem Transport von E-Mails und anderer Nachrichten handelt es sich in der Regel um Telekommunikationsdienste, so dass hierbei das Fernmeldegeheimnis gilt. Wird im Online-Spiel (vorgelagert) das Schreiben der Nachricht und (nachgelagert) das Lesen angeboten, so handelt es sich hierbei um Telemediendienste.

Der Spiele-Betreiber darf grundsätzlich keine Einsicht in die private Kommunikation zwischen

den Spielern nehmen. Dies gilt auch für den Administrator bei der Wartung der Systeme. Eine Kenntnisnahme ist bei ihm im Rahmen des technisch Möglichen zu unterbinden. Kann dieses technisch etwa durch Verschlüsselung der Inhalte nicht verhindert werden, so ist er auf jeden Fall besonders auf seine datenschutzrechtlichen Pflichten hinzuweisen, und ggf. ist eine manipulationsfeste bzw. revisionssichere Protokollierung seiner Zugriffe auf Nachrichten vorzusehen.

Die automatische Analyse der Nachrichten zur Untersuchung auf Schadsoftware oder Spam kann zulässig sein, wenn die Spieler hierauf hingewiesen wurden. Der Absender und eventuell der Empfänger sind darüber zu informieren, wenn eine Nachricht aufgrund der automatischen Analyse nicht zugestellt werden konnte.

Unter das Fernmeldegeheimnis fallen neben den Nachrichteninhalten auch die weiteren Umstände der Kommunikation, wie etwa die betroffenen Kommunikationspartner. Derartige Daten dürfen in der Regel auch nicht über Sicherheitszwecke hinaus protokolliert werden (vgl. Abschnitt 9.2.4)

Für Anbieter der elektronischen Post galt bis zum Urteil des Bundesverfassungsgerichts vom 2. März 2010[114] zunächst die Pflicht zur Vorratsdatenspeicherung nach § 113a Abs. 1 und 3 TKG. Danach hatten die Anbieter folgende Daten für sechs Monate aufzubewahren:

aa) bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

bb) bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

cc) bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

dd) die Zeitpunkte der bei 1) bis 3) genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Der Telekommunikationsdiensteanbieter hatte die allein auf Grund der Vorratsdatenspeicherung gespeicherten Daten innerhalb eines Monats nach Ablauf sechs Monate zu löschen oder die Löschung sicherzustellen (§ 113a Abs. 11 TKG). Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht die konkreten Regelungen der Vorratsdatenspeicherung für nicht verfassungsgemäß angesehen, so dass u. a. die Regelung des § 113a TKG nichtig ist. Allerdings muss auch Deutschland die EU-Richtlinie zur Vorratsdatenspeicherung 2006/24/EG damit noch umsetzen, so dass entsprechende Regelungen in nächster Zeit zu erwarten sind.

[114] Az.: 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

d) Mögliche Lösungen

- Vorgehaltene persönliche Nachrichten / E-Mails sind möglichst nur verschlüsselt auf dem Server abzulegen, so dass die Administratoren keine Einsicht nehmen können.
- Zugriffe der Administratoren auf Nachrichten sollten protokolliert werden, so dass ein Aufdeckungsrisiko für Personen besteht, die unbefugt Zugriff auf Nachrichten nehmen.
- Es dürfen grundsätzlich keine Protokolle von Nachrichteninhalten und Informationen über Absender und Empfänger erstellt werden.
- Es sollte eine Beschwerdemöglichkeit für die Spieler eingerichtet werden, über die unwillkommene Nachrichten dem Betreiber gemeldet werden können.
- Die angewendeten Verfahren, Löschungsfristen und Zugriffsmöglichkeiten sollten durch entsprechende Dokumentationen für den Betreiber transparent sein.
- Ist eine automatisierte Kontrolle der Nachrichten auf Spam bzw. Schadsoftware geboten, so hat diese nach den üblichen technischen Methoden zu erfolgen und darf kein persönlicher Zugriff durch z. B. die Administratoren erfolgen. Über gefilterte Nachrichten sind der Absender und der Empfänger zur unterrichten.
- Die Einsichtnahme in Nachrichten darf nur mit Einwilligung der betroffenen Kommunikationspartner erfolgen.
- Ordnungsbehörden dürfen in der Regel nur dann Zugriff auf Nachrichten erhalten, wenn ein entsprechender richterlicher Beschluss vorliegt.
- Eine Vorratsdatenspeicherung zum Zwecke der Strafverfolgung gibt es (zur Zeit) nicht, so dass diese im Falle einer Implementierung beim Betreiber rechtswidrig wäre.

9.2.15 Datenschutzkonfiguration

a) Funktionalitätsbeschreibung

Den Spielern kann innerhalb des Online-Spiels die Möglichkeit gegeben werden, selber einzustellen, wie mit ihren personenbezogenen Daten verfahren wird. Dies umfasst beispielsweise Speicherfristen, Art und Umfang der zu verarbeitenden Daten oder eine mögliche Weitergabe von Daten an Dritte bzw. Mitspieler.

b) Relevante Normen

- §§ 4a, 28 Abs. 3b BDSG
- §§ 13 Abs. 2 und Abs. 3 TMG

c) Restriktionen

Soll aus einer Datenschutzkonfiguration eine Einwilligung für die Verarbeitung von Daten abgeleitet werden, so muss diese bewusst und eindeutig erklärt werden. Der Spieler muss über die Konsequenzen der Konfiguration aufgeklärt werden. Eine Einwilligung kann in der Regel nicht aus dem Umstand heraus fingiert werden, dass eine Konfiguration nicht geändert

wurde. Die Vornahme einer Einstellung darf nicht dafür ausschlaggebend sein, ob das Spiel gespielt werden kann oder nicht.

d) Mögliche Lösungen

- Dem Nutzer ist so weit wie möglich selbst die Entscheidung darüber zu lassen, wie mit seinen personenbezogenen Daten verfahren wird.
- Voreinstellungen bzgl. des Datenschutzes sind so restriktiv wie möglich zu wählen. Dies gilt insbesondere für minderjährige Spieler.
- Werden Konfigurationen nicht restriktiv gewählt, so ist der Spieler zu Beginn der Nutzung des Online-Spiels hierüber zu informieren und darauf hinzuweisen, wo er Änderungen vornehmen kann.
- Der Spieler ist vor der Vornahme einer Konfiguration darüber zu informieren, was die Einstellungen bewirken.
- Werden im Nachhinein Konfigurationsmöglichkeiten verändert, so ist der Spieler hierüber zu unterrichten.
- Soll die Wirkungsweise einer Konfiguration bzgl. des Datenschutzes erweitert werden (z. B. Ausweitung der Weitergabe von Daten), so darf dieses nur erfolgen, wenn der Spieler ausdrücklich eingewilligt hat.

9.2.16 Datenschutzerklärung

a) Funktionalitätsbeschreibung

Werden von einem Spiel personenbezogene Daten verarbeitet, so ist der Spieler u. a. durch eine Datenschutzerklärung hierüber zu informieren.

b) Relevante Normen

- § 13 Abs. 1 TMG

c) Restriktionen

Der Betreiber hat den Spieler zu Beginn der Nutzung des Spiels über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu unterrichten. Dies schließt auch die Wahl- und Gestaltungsmöglichkeiten des Spielers ein. Werden Daten außerhalb der EU verarbeitet, so ist auch dieses in die Datenschutzerklärung aufzunehmen. Die Unterrichtung hat in allgemein verständlicher Form zu erfolgen. Werden Cookies oder andere den Spieler später wieder identifizierende Merkmale automatisiert eingesetzt, so ist der Spieler auch hierüber zu Beginn des Verfahrens, in der Regel nach aktuellem Recht in der Datenschutzerklärung, zu informieren. Der Inhalt der Unterrichtung muss für den Spieler jederzeit abrufbar sein.

Bei Spielsystemen, die Sozialen Netzwerken ähneln, muss nach Ansicht der Aufsichtsbehörden auch über Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind, aufgeklärt werden. Darüber hinaus haben die Betreiber ihre Nut-

zer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

d) Mögliche Lösungen

- Die Datenschutzerklärung muss schon bei der Installation des Spiels bzw. bei der Registrierung dem Spieler gezeigt werden, wobei der Spieler aktiv mittels eines Klicks bestätigt, dass er die Datenschutzerklärung zur Kenntnis genommen hat.
- Bei einem Browserspiel muss die Datenschutzerklärung direkt von der Startseite aufrufbar sein.
- Gestaltung der Datenschutzerklärung in allgemein verständlicher deutscher Sprache, wobei auf komplizierte Rechtsausführungen verzichtet werden sollte.
- Präsentation der Datenschutzerklärung in mehreren Ebenen (sog. „Layern“). So werden zunächst nur die Hauptpunkte der Erklärung grob umrissen. Zu jedem Punkt besteht dann eine Möglichkeit zur Anzeige weiterer Informationen.
- Die Datenschutzerklärung sollte mit Datum und Versionsnummer versehen werden. Änderungen zur vorherigen Version sollten kenntlich gemacht und den Spielern vor Inkrafttreten mitgeteilt werden.
- Die Darstellung zum Einsatz von Cookies sollte auch Informationen dazu enthalten, was Cookies sind und wie man ihren Einsatz unterbinden kann.
- Die Darstellung des Zwecks muss so genau wie möglich sein. Pauschale Ausdrücke wie „zur Erbringung des Spiels“ sind in der Regel nicht ausreichend.
- Es sollte herausgestellt werden, welche Daten unbedingt für die Nutzung des Spiels erforderlich sind und welche vom Spieler optional eingegeben werden können.
- Die Datenschutzerklärung sollte eine Kontaktmöglichkeit beinhalten, an die sich der Spieler bei Fragen oder auch für Löschungs-, Auskunfts-, und Berichtigungswünschen wenden kann.
- Der Spieler ist auf seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung hinzuweisen und wie er diese erreichen kann. Dies betrifft auch die Realisierung der Möglichkeit der Rücknahme einer Einwilligung.
- Der Spiele-Betreiber hat die Verantwortung dafür, organisatorisch sicherzustellen, dass die Rechte des Spielers auf Auskunft, Berichtigung, Löschung und Sperrung umgesetzt werden. Die Bestellung eines betrieblichen Datenschutzbeauftragten als Ansprechpartner ist sinnvoll, entbindet die Unternehmensleitung aber nicht von der Verantwortlichkeit.

e) Weiterführende Literatur

- Artikel 29-Datenschutzgruppe: Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten: http://www.cnpd.lu/objets/wp29/wp100_de_pdf.pdf.

9.2.17 Weiterleitung von Daten an Dritte

a) Funktionalitätsbeschreibung

Es kann für den Betreiber eines Online-Spiels gewollt sein, Daten an Dritte weiterzugeben. Dies kann dazu geschehen, um bestimmte Tätigkeiten auszulagern (z. B. Statistikerstellung oder Abrechnung) oder um diesen eigene Dienste zu ermöglichen (z. B. weitere Spiele oder Werbung).

b) Relevante Normen

- §§ 4, 4a, 4b, 4c, 11, 28 BDSG
- §§ 12, 13 TMG

c) Restriktionen

Es ist zu unterscheiden:

aa) Beauftragung eines Dritten mit Datenverarbeitung (Auftragsdatenverarbeitung)

In diesem Fall bleibt der Auftraggeber verantwortliche Stelle. Notwendig ist ein schriftlicher Vertrag, der die in § 11 Abs. 2 BDSG aufgeführten Punkte enthält. Dabei hat sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Dies ist zu dokumentieren. Eine Auftragsdatenverarbeitung kommt nur dann in Betracht, wenn der Auftragnehmer entsprechend den Weisungen des Auftraggebers handelt und der Auftragnehmer kein Eigeninteresse an den Daten hat (etwa zur Vermischung mit Daten anderer Auftraggeber bzw. eigene Geschäftszwecke). Hat der Auftragnehmer seinen Sitz außerhalb der EU und in einem Land, das kein zur EU anerkanntes vergleichbares Datenschutzniveau aufweist, so scheidet in der Regel eine Auftragsdatenverarbeitung gänzlich aus.

bb) Weitergabe personenbezogener Daten außerhalb einer Auftragsdatenverarbeitung

In Fällen außerhalb der Auftragsdatenverarbeitung liegt in der Regel eine Funktionsübertragung bzw. eine Übermittlung vor. In diesem Fall muss in den meisten Fällen eine Einwilligung des Betroffenen in die Weitergabe vorliegen. Ausnahmen gibt es u. a. für die Bereiche Abwehr von Gefahren, Verfolgung von Straftaten, wissenschaftliche Forschung und sehr eingeschränkt für den Adresshandel (§ 28 Abs. 3 BDSG) und – zur Wahrung berechtigter Interessen – für Auskunfteien (§ 29 BDSG).

d) Mögliche Lösungen

- Wenn möglich, ist ein Vertrag über die Auftragsdatenverarbeitung nach Maßgabe des § 11 BDSG zu schließen.
- Sodann ist die Einhaltung der Datenschutzmaßnahmen regelmäßig durch den Auftraggeber beim Auftragnehmer zu überprüfen und zu dokumentieren.
- Übermittlung von personenbezogenen Daten an Dritte darf in der Regel nur mit Einwilligung des Betroffenen erfolgen. Hierbei darf die Bereitstellung des Spiels nicht von der

Einwilligung abhängig gemacht werden. Außerdem muss der Einwilligende darüber informiert werden, an wen die Daten weitergegeben werden und für welchen Zweck.

- Sofern eine Einwilligung vorliegt, muss die Stelle, an die die Daten übermittelt werden, über die Zweckbindung der Daten informiert werden.
- Da IP-Adressen als personenbeziehbare Daten angesehen werden, stellt auch deren Übermittlung an Dritte (z. B. Analyseanbieter oder Werbeanbieter) eine Übermittlung dar, die in der Regel eine Einwilligung erfordert. Eine Auftragsdatenverarbeitung ist auch hier nur denkbar, wenn beim Auftragnehmer kein Eigeninteresse an den Daten besteht.

e) Weiterführende Literatur

- Hinweise des ULD zum Thema Tracking: https://www.datenschutzzentrum.de/tracking/.
- Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund über „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“: http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf.

9.2.18 In-Game-Advertising

a) Funktionalitätsbeschreibung

Wird innerhalb eines Online-Spiels Werbung eingeblendet, so kann diese von vornherein eingebaut sein oder aber fallbezogen nachgeladen werden. Hierbei kann die Werbung vom Betreiber / Hersteller des Spiels eingebunden werden oder direkt vom Werbetreibenden oder einer Vermarktungsgesellschaft stammen.

b) Relevante Normen

- §§ 6, 12, 13 Abs. 5 und Abs 6, 15 TMG
- § 28 BDSG

c) Restriktionen

Bei Werbung in Online-Spielen handelt es sich in der Regel um sog. „kommerzielle Kommunikation“ i. S. d. § 6 TMG. Diese muss klar als solche erkennbar, der Auftraggeber muss identifizierbar und Preisnachlässe, Zugaben, Geschenke, Preisausschreiben sowie Gewinnspiele müssen mit ihren Bedingungen deutlich sein.

Werden Statistiken über die Einblendung bzw. das Aufrufen von Werbung erstellt, so dürfen dabei verwendete Profile nur unter Pseudonym gespeichert und dem Spieler muss ein Widerspruchsrecht eingeräumt werden. Die vollständige IP-Adresse darf nicht für die Analyse des Nutzerverhaltens herangezogen werden. Werden personenbezogene Daten über die Spieler an Dritte (insbes. die Werbetreibenden) weitergegeben, ist hierfür die ausdrückliche Einwilligung des Spielers erforderlich. Dies gilt in der Regel schon dann, wenn nur die IP-Adresse des Spielers an den Werbetreibenden übermittelt wird, damit dieser die Werbung in das Spiel einblenden kann.

d) Mögliche Lösungen

- Der Betreiber sollte möglichst die Werbung an den Spieler selber übermitteln und nicht über einen Dritten.
- Der Spieler wird vor dem Start des Spiels darüber informiert, dass Profile erstellt werden, die für Werbezwecke genutzt werden. Sind diese Profile unmittelbar mit seinem Namen / Adresse / IP-Adresse verknüpft, so ist die Einwilligung des Spielers hierfür erforderlich. Werden nur Profile unter Verwendung von Pseudonymen für die Werbung genutzt, so ist dem Spieler ein Widerspruchsrecht einzuräumen.
- Der Spieler sollte wählen können, ob er personalisierte Werbung erhalten möchte oder nicht.
- Werden Informationen des Spielers zu Werbezwecken an Dritte übermittelt, so ist in der Regel die ausdrückliche Einwilligung des Spielers vorher einzuholen. Dabei ist darauf hinzuweisen, an wen die Daten übermittelt werden und zu welchem Zweck dies geschieht.
- Sollen Daten an Dritte übermittelt werden, die Rückschlüsse auf den Gesundheitszustand des Spielers erlauben (z. B. Gewicht, Jogginggewohnheiten), so ist hierfür eine besondere ausdrückliche Einwilligung einzuholen, die sich explizit auf diese Daten bezieht. Möglichst ist ganz auf die Übermittlung dieser Daten zu verzichten.

9.2.19 Altersverifikation und Jugendschutz

a) Funktionalitätsbeschreibung

Richtet sich ein Online-Spiel an Spieler ab einem gewissen Alter, so muss dieses Alter in der Regel durch den Betreiber überprüft werden. Dies gilt insbesondere für Spiele, deren Verwendung nur Erwachsenen erlaubt ist.

b) Relevante Normen

- Jugendmedienstaatsvertrag
- § 14 TMG
- § 4 PersAuswG

c) Restriktionen

Die für die Altersverifikation gespeicherten Daten sind auf diejenigen personenbezogenen Daten zu beschränken, die für die Verifikation erforderlich sind. Ist ein umfassender Altersnachweis von den Gesetzen nicht vorgeschrieben, so kann dieses ggf. die Beschränkung auf die Bestätigung der entsprechenden Altersgrenze bedeuten, ohne dass das genaue Geburtsdatum genannt werden muss. Wird für die Altersverifikation der Personalausweis verwendet (etwa weil es sich um ein Spiel handelt, das für Jugendliche nicht freigegeben ist), so gilt, dass die Seriennummer nicht so verwendet werden darf, dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Der

Personalausweis darf weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden. Wird die Einsendung der Kopie eines Personalausweises verlangt, so ist diese nach Feststellung der Identität bzw. des Alters in der Regel umgehend zu vernichten, da dann der Zweck für die Datenerhebung entfällt und keine Erforderlichkeit mehr besteht.

d) Mögliche Lösungen

- Soweit möglich, ist auf die Erhebung des genauen Geburtsdatums zu verzichten und es sollte nur die Information gespeichert werden, ob eine Person die Altersgrenze überschreitet.
- Auf die Erstellung von Ausweiskopien ist so weit wie möglich zu verzichten bzw. diese ist nach der Altersverifikation umgehend zu vernichten.
- Die Seriennummer des Ausweises darf nicht für die spätere Wiedererkennung einer Person gespeichert werden.

9.2.20 Suchtprävention

a) Funktionalitätsbeschreibung

Für die Suchtprävention kann ein Bedarf daran bestehen, dass Personen von der Nutzung eines Spiels langfristig ausgeschlossen werden. Hierfür können dann ggf. Sperrlisten erforderlich sein. Dabei kann sowohl für die Betreiber ein Interesse an der Sperrung von Spielern bestehen, wie aber auch Spieler zum Selbstschutz wünschen können, nicht mehr für ein Spiel zugelassen zu werden.

b) Relevante Normen

- § 13 Abs. 2 TMG
- § 4a BDSG
- § 8 Glücksspielstaatsvertrag

c) Restriktionen

Möchte ein Spieler für ein Spiel gesperrt werden, so ist hierfür seine ausdrückliche Einwilligung erforderlich. Bei Jugendlichen kann eine Sperrung auch durch die Eltern erklärt werden, wobei zu beachten ist, dass diese Sperre durch den Jugendlichen in der Regel ab Vollendung seines 18. Geburtsjahres selber wieder aufgehoben werden kann. Im Bereich der Glückspiele im Sinne des Glücksspielstaatsvertrages ist ein Sperrsystem einzuführen, bei dem eine Entsperrung des Spielers frühestens nach einem Jahr erfolgen darf. Der Betreiber eines sonstigen Online-Spiels hat in der Regel eine Löschung des Spielers von der Sperrliste ab Widerruf der Einwilligung vorzunehmen.

d) Mögliche Lösungen

- Für den Eintrag auf einer Sperrliste zur Suchprävention ist die Einwilligung des Spielers einzuholen.

- Wünscht der Spieler außerhalb des Anwendungsbereichs des Glücksspielstaatsvertrages die Löschung von der Sperrliste, so hat dieses in der Regel umgehend zu erfolgen.
- Die Daten auf den Sperrlisten dürfen nur für die Sperrung eines Spielers verwendet werden. Eine Weitergabe der Sperrliste außerhalb des Anwendungsbereichs des Glücksspielstaatsvertrages ist nur mit der Einwilligung der betroffenen Spieler möglich.
- Dem Spieler sollte bei Erteilung der Einwilligung in die Eintragung auf einer Sperrliste mitgeteilt werden, welche Daten dort erfasst werden und wie er die Einwilligung widerrufen kann.
- Auf Wunsch ist dem Spieler jederzeit Auskunft darüber zu erteilen, welche Daten von ihm auf der Sperrliste erfasst sind.

9.2.21 (In-Game-)Shopping

a) Funktionalitätsbeschreibung

Online-Spiele können den Spielern ermöglichen, innerhalb des Spiels virtuelle oder reale Produkte zu kaufen. Zumeist sind diese Erweiterungen für das Spiel bzw. zusätzliche Inhalte.

b) Relevante Normen

- §§ 3a, 4a, 28 BDSG
- Nr. 8 Anlage zu § 9 Satz 1 BDSG
- §§ 13 Abs. 5 und 6 TMG

c) Restriktionen

Die Daten, die zum Zweck des In-Game-Shoppings erhoben werden, müssen so weit wie möglich getrennt von den sonstigen Spielerdaten verarbeitet werden. Es sind so wenig personenbezogene Daten wie möglich zu erheben. Soweit technisch möglich und zumutbar ist eine anonyme Bezahlung zu ermöglich. Wird der In-Game-Shop durch einen Dritten betrieben, so ist die Weitervermittlung dem Spieler anzuzeigen. Eine Übermittlung von personenbezogenen Daten durch den Spiel-Betreiber an den Shop-Betreiber ist in der Regel nur mit Einwilligung des Spielers zulässig.

d) Mögliche Lösungen

- Dem Spieler ist die Nutzung und die Bezahlung beim Shopping in pseudonymer bzw. anonymer Form anbieten, etwa durch Nutzung von Prepaid-Karten.
- Die von dem Shop erhobenen Daten sind auf die zur Vertragserfüllung und zum Inkasso erforderlichen Angaben zu beschränken. Bei Prepaid-Zahlung und Online-Auslieferung ist die Erhebung personenbezogener Daten regelmäßig nicht erforderlich.
- Die beim Shopping notwendigerweise erhobenen Daten sind nach Wegfall der Erforderlichkeit zu löschen. An Stelle des Löschens tritt die Sperrung in den Fällen, in denen eine Aufbewahrungspflicht z. B. durch die Abgabenordnung bzw. das Handelsgesetzbuch be-

steht. Dann müssen die (Rechnungs-)Daten jedoch aus dem aktiven System ausgesondert werden.

- Wird an einen externen Shop-Betreiber weitervermittelt, so ist diese Vermittlung dem Spieler deutlich schon vor der Weiterleitung kenntlich zu machen.

9.2.22 In-Game-Verhaltensanalyse

a) Funktionalitätsbeschreibung

Spiele-Betreiber können ein Interesse daran haben, das Spielerverhalten zu analysieren, um das Spiel zu optimieren, Werbung bedarfsgerecht zu platzieren oder den Erfolg eines Spiels oder bestimmter Spielteile zu ermitteln, z. B. in Form einer Statistik.

b) Relevante Normen

- §§ 13, 15 TMG
- § 11 BDSG

c) Restriktionen

Rein statistische Erhebungen, die keinen Personenbezug ermöglichen, sind zulässig. Der Spiele-Betreiber darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Spiels Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Spieler dem nicht widerspricht. Der Betreiber hat den Spieler auf sein Widerspruchsrecht im Rahmen der Datenschutzerklärung hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. IP-Adressen sind nach herrschender Meinung keine Pseudonyme, die für solche Profile verwendet werden dürfen. Daher dürfen sie ohne Einwilligung nur auf eine Weise bei der Profilerstellung genutzt werden, dass ein Personenbezug ausgeschlossen ist. Dies gilt auch für das Geotargeting (Bestimmung des Ortes, an dem sich der Anschluss befindet), das ebenfalls ohne Einwilligung nicht mit vollständigen IP-Adressen durchgeführt werden darf.

Wird ein dritter Dienstleister mit der Verhaltensanalyse beauftragt, so ist in der Regel ein Auftragsdatenverarbeitungsverhältnis inkl. Vertrag i. S. d. § 11 BDSG erforderlich, sofern keine Einwilligung des Spielers für eine Übermittlung vorliegt. Der Auftragnehmer darf bei einer Auftragsdatenverarbeitung kein Eigeninteresse an den Daten haben.

Für eine vorauseilende Speicherung von Daten über die Nutzung des Online-Spiels hinaus, beispielsweise zu Zwecken einer eventuellen zukünftigen Strafverfolgung, besteht keine Rechtsgrundlage.

d) Mögliche Lösungen

- Es wird eine rein statistische Auswertung erstellt, ohne dass ein Rückschluss auf einzelne Spieler möglich ist.
- IP-Adressen werden anonymisiert bzw. pseudonymisiert. Dies kann z. B. durch Löschung der letzten beiden Oktette erfolgen.

- Für ein Geotargeting sollen nur entsprechend gekürzte IP-Adressen verwendet werden.
- Die Spielerprofile müssen unter Pseudonym gespeichert werden, wobei die Zuordnung zum Pseudonym getrennt von den Profilen aufbewahrt und eine Zusammenführung so weit wie möglich technisch ausgeschlossen werden.
- In die Datenschutzerklärung wird eine Unterrichtung über die Widerspruchsmöglichkeit gegen die Profilerstellung aufgenommen.
- Es sollte ggf. auf externe Dienstleister verzichtet und die Profilerstellung selber als Betreiber vornehmen werden.
- Bei Einbindung eines externen Dienstleisters ist zu beachten, dass weitergehende Beschränkungen gegeben sein können, wenn dieser die Daten außerhalb der EU (oder einem Land mit anerkanntermaßen vergleichbaren Datenschutzgrundsätzen) verarbeitet.
- Die Löschung des Verhaltensprofils sollte dem Nutzer möglich sein. Bei einem Pseudonymwechsel sollte ein neues, leeres Verhaltensprofil angelegt werden.
- Auch hinsichtlich pseudonymisierter Profile haben die Betroffenen ein Auskunftsrecht gegenüber der Daten verarbeitenden Stelle, das organisatorisch beim Betreiber umgesetzt werden muss.

9.2.23 Webcam / Videoaufzeichnung

a) Funktionalitätsbeschreibung

Webcams können bei Online-Spielen dazu dienen, Mitspieler bei der Kommunikation auf dem Bildschirm zu sehen. Des Weiteren können sie dazu eingesetzt werden, um z. B. ein Bild des Spielers auf eine Spielfigur zu projizieren oder eine Steuerung des Spiels mittels Bewegung zu ermöglichen.

b) Relevante Normen

- §§ 3a, 4a BDSG
- § 15 TMG
- § 22 KunstUrhG

c) Restriktionen

Für den Spieler muss bei Verarbeitung von Bilddaten außerhalb seines Spielsystems stets erkennbar sein, ob er von der Kamera gerade erfasst wird und wohin diese Daten übertragen werden. Derartige Bilder dürfen nur mit seiner Einwilligung weiterverarbeitet bzw. verbreitet und veröffentlicht werden.

Videochatinhalte dürfen für den Fall, dass sie nicht für jedermann einsehbar sind, grundsätzlich nicht unbefugt überwacht oder protokolliert werden. Für eine automatisierte oder manuelle Überwachung der Videoinhalte und für deren Protokollierung zur späteren Analyse ist die Einwilligung aller Teilnehmer erforderlich. Richtet sich der Dienst an Kinder bzw. Jugendli-

che, so kann es aus Jugendschutzgründen erforderlich sein, eine Moderation durchzuführen. Dies kann z. B. der Fall sein, wenn das Spiel die Gefahr beinhaltet, dass Kinder (sexuell) belästigt werden. Die Moderation muss jedoch für alle Teilnehmer ersichtlich sein. Ist in einem Video-Chat ein Moderator anwesend, der bei Verstößen gegen die Chatregeln eingreifen kann, so ist dieser als solcher kenntlich zu machen (siehe auch Abschnitt 9.2.13).

d) Mögliche Lösungen

- Die Videokamera sollte mit einer LED ausstattet werden, die leuchtet, wenn Videobilder an Dritte übertragen werden. Zusätzlich sollte dies auch auf dem Bildschirm angezeigt werden.
- Für die Übertragung von Videobildern muss die ausdrückliche Einwilligung des Spielers eingeholt werden.
- Bei der Verarbeitung von Videobildern ist auch zu beachten, dass ggf. Personen das Spielsystem nutzen, die sich zuvor nicht selber registriert haben. Somit ist es ratsam, vor jeder Aktivierung der Übertragung von Videodaten an Dritte einen Hinweis anzuzeigen.
- Es ist eine einfache Möglichkeit zu integrieren, um eine Videoübertragung umgehend zu unterbrechen.
- Es ist Transparenz darüber zu schaffen, wer Einsicht in einen Videochat hat (z. B. nur zugelassene Personen oder jeder).
- Soll eine Moderation / Protokollierung durchgeführt werden, so sind die Teilnehmer zuvor hierüber zu informieren, und es ist eine Einwilligung einzuholen.
- Bei Angeboten, die sich an Kinder / Jugendliche richten, kann eine Moderation geboten sein. Diese muss jedoch transparent sein.
- Anstelle der Überwachung / Protokollierung kann ggf. als milderes Mittel die Möglichkeit eingebaut werden, sich über Chatteilnehmer zu beschweren. Hierzu sollte ein entsprechendes Beschwerdemanagement eingerichtet werden.
- Protokolle sind nach Wegfall der Erforderlichkeit umgehend zu löschen. Die Erforderlichkeit entfällt z. B. im Fall des Zwecks „Schutz der Videochatteilnehmer“ dann, wenn mit der Meldung einer Beschwerde nicht mehr gerechnet werden kann (z. B. nach sieben Tagen). Die Löschfristen sind den Spielern im Rahmen der Datenschutzerklärung mitzuteilen.
- Der Zugriff auf die Webcam sollte technisch so gestaltet sein, dass ein Missbrauch so weit wie möglich ausgeschlossen ist.
- Im Rahmen des technisch Möglichen sollte unterbunden werden, dass Kommunikationspartner das Videobild mitschneiden können, wobei Spieler darüber informiert werden sollten, dass dieses nie völlig ausgeschlossen werden kann. Soll dieses gerade ermöglicht werden, so müssen hierüber alle teilnehmenden Kommunikationspartner informiert werden und eingewilligt haben.

9.2.24 Always-Online-Funktionalität

a) Funktionalitätsbeschreibung

Insbesondere Konsolen und Handys können die Funktion beinhalten, stets online zu sein, um Nachrichten zu empfangen oder weiterzuversenden.

b) Relevante Normen

- §§ 13, 15 TMG

c) Restriktionen

Die Always-Online-Funktionen sind transparent zu gestalten. Hierbei muss dem Spieler mitgeteilt werden, welche Art Daten in welchem Umfang und für welchen Zweck verarbeitet bzw. an wen wann übermittelt werden. Insbesondere ist zu vermeiden, dass hierüber das Alltagsverhalten eines Spielers analysiert wird (z. B. Schlafenszeiten, Arbeitstage, Urlaube) und sich Rückschlüsse über seine Lebensverhältnisse ergeben (Anzahl der Personen in einem Haushalt etc.). Hierbei handelt es sich im Zusammenhang mit den Zugangsdaten des Spielers um personenbezogene Daten, die den Datenschutzgesetzen unterliegen.

d) Mögliche Lösungen

- In die Datenschutzerklärung müssen Informationen darüber aufgenommen werden, welche Daten in welchem Umfang und warum verarbeitet werden.
- Der Spieler muss die Möglichkeit haben, die Verbindung zu unterbrechen. Es muss somit eine Abschaltmöglichkeit vorhanden sein.
- Werden auch im Offline-Modus Daten über das Spielverhalten gesammelt und bei einer späteren Aktivierung der Online-Funktion übertragen, so ist hierfür die Einwilligung des Spielers einzuholen. Liegt diese nicht vor, muss die Übertragung unterbleiben.
- Die Übertragung sollte für den Spieler stets transparent gestaltet werden bzw. nachvollziehbar sein.
- Es ist bei der Profilerstellung zu verhindern, dass über die Always-Online-Funktionen das häusliche Verhalten, Urlaubszeiten etc. nachvollziehbar sind. Informationen über Einschaltzeiten, Bewegungsmuster (Mobilfunk) etc. dürfen nur mit Einwilligung verarbeitet werden. Sie sind dann so früh wie möglich zu löschen / zu anonymisieren. Möglichst ist vollständig auf die Verarbeitung solcher Informationen zu verzichten.

9.2.25 Mobile-Gaming

a) Funktionalitätsbeschreibung

Portable Spielkonsolen und Handys ermöglichen das Spielen an fast jedem Ort. Es werden in der Regel Mobilfunknetze oder WLAN-Netze für das Online-Spielen verwendet. Einige Spiele bauen hierbei auch die Standortdaten des Spielers mit in das Spielgeschehen ein oder erfassen diese aus anderen Gründen (z. B. zur Regionalisierung der Spielsoftware oder

Spracheinstellung).

b) Relevante Normen

- § 98 TKG
- § 13 Abs. 4 Nr. 3 TMG

c) Restriktionen

Bei der Nutzung von Mobilfunk- oder WLAN-Netzen ist es Aufgabe des Betreibers von Online-Spielen, die Kenntnisnahme der übertragenen Daten durch unberechtigte Dritte so weit wie technisch möglich und zumutbar zu verhindern.

Standortdaten, die in Bezug insbesondere auf Mobilfunknetze oder WLAN-Stationen verwendet werden, dürfen nur im zur Bereitstellung des Online-Spiels erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Spieler seine Einwilligung erteilt hat. Werden die Standortdaten für ein Online-Spiel verarbeitet, das die Übermittlung von Standortdaten eines Mobilfunkendgerätes an andere Teilnehmer oder Dritte, die nicht Betreiber des Spiels sind, zum Gegenstand hat, muss der Teilnehmer seine Einwilligung ausdrücklich, gesondert und schriftlich erteilen. In diesen Fällen hat der Betreiber des Spiels den Spieler nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren, es sei denn, der Teilnehmer hat gemäß § 95 Abs. 2 Satz 2 TKG widersprochen. Der Spieler muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Hierauf sollte ihn der Betreiber hinweisen. Eine Einwilligung kann jederzeit widerrufen werden.

Haben die Spieler ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen. Die Verarbeitung von Standortdaten muss auf das für die Bereitstellung des Online-Spiels erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der das Online-Spiel anbietet, handeln.

d) Mögliche Lösungen

- Es sollten Verschlüsselungsmethoden für die Übertragung von Spieldaten (z. B. SSL) verwendet werden. Können portable Spielkonsolen über WLAN Verbindung mit dem Internet aufnehmen, so sollte die Konsole zumindest eine aktuelle WPA-Verschlüsselung unterstützen.
- Über die Verarbeitung von Standortdaten sowohl bei Nutzung von Mobilfunk- als auch WLAN-Netzen sind dem Spieler die sich aus § 98 TKG ergebenen Informationen zu übermitteln und Einwilligungen einzuholen.

e) Weiterführende Literatur

- Zur Verwendung von Standortdaten zur Erbringung des Services: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf.
- Zu Besonderheiten von auf Standortdaten beruhendem Marketing: http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis-wp11-del11.12_mobile_marketing_in_the_perspective_of_identity_privacy_and_transparency.pdf.

9.2.26 Spielen über Internet

a) Funktionalitätsbeschreibung

Online-Spiele können zum Datenaustausch mit dem Spielserver oder mit Mitspielern das Internet einsetzen. Hierbei fällt insbesondere als personenbeziehbares Datum die IP-Adresse an.

b) Relevante Normen

- §§ 13, 15 TMG

c) Restriktionen

Die Speicherfristen und Verwendungsmöglichkeiten für IP-Adressen richten sich nach dem Speicherzweck:

- Zur Ermöglichung des Spiels: Nur solange das Spiel gespielt wird.
- Zu Abrechnungszwecken: Je nach Abrechnungszeitraum und Einwendungsfristen – maximal bis sechs Monate nach Rechnungsstellung. Wurde vom Spieler eine Einwendung erhoben (z. B. Bestreiten einer Geldforderung), so verlängert sich diese Frist bis zur Erledigung der Einwendung.
- Aus Sicherheitsgründen (z. B. Identifikation von Denial of Service- oder Hacking-Angriffen): Maximal sieben Tage.
- Zur Erstellung von Statistiken / Profilerstellung: Eine Speicherung der IP-Adresse ist nicht zulässig ist. Dies betrifft insbesondere Logfiles von Spielservern. Sollen IP-Adressen in diesen Logfiles für Statistikzwecke / Profilerstellung verwendet werden, so müssen sie vorher so anonymisiert (z. B. gekürzt) werden, dass ein Rückschluss auf die ursprüngliche IP-Adresse ausgeschlossen ist. Auf dieser Datenbasis sind rein statistische Auswertungen zulässig. Werden IP-Adressen im Rahmen der Anonymisierung durch Pseudonyme ersetzt, so ist sicherzustellen, dass keine Möglichkeit besteht, die ursprüngliche IP-Adresse zu bestimmen oder durch das Zusammenspiel mit weiteren Daten eine Identifizierung des Nutzers vorzunehmen.

Zu beachten ist des Weiteren, dass der Spiele-Betreiber den Spieler zu Beginn über Umfang und Zweck der Verarbeitung der IP-Adresse aufklären muss. Dies erfolgt in der Regel in der

Datenschutzerklärung des Online-Spiels (siehe Abschnitt 9.2.16).

Der Betreiber hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Spieler das Online-Spiel geschützt gegen Kenntnisnahme unberechtigter Dritter in Anspruch nehmen kann. Möglichst ist somit die Online-Verbindung zu verschlüsseln.

d) Mögliche Lösungen

- In Logfiles ist so weit wie möglich auf personenbeziehbare Daten (insbesondere IP-Adressen) zu verzichten. In der Praxis sind die IP-Adressen unverzüglich durch ein nicht zurück auflösbares Kennzeichen zu ersetzen. Sowohl für Apache als auch Microsoft Internet Information Server existiert Software, die diese Anonymisierung automatisch vornehmen kann. Beispiele finden Sie hier: http://www.saechsdsb.de/ipmask/.
- Auch der Referer kann ggf. personenbezogene Daten enthalten (z. B. wenn Nutzernamen / Formulareinträge über Argumente an den Webserver übermittelt werden) und sollte dann nicht länger aufbewahrt werden, als für die Erbringung des Spiels erforderlich.
- Eine längere Speicherfrist für IP-Adressen ist zu Abrechnungszwecken und Sicherheitszwecken ggf. zulässig (s. o.). Die Unterrichtungspflicht des Spiele-Betreibers nach § 13 Abs. 1 TMG ist zu beachten.
- Analysen des Nutzungsverhaltens mit ungekürzten IP-Adressen sind in der Regel nur mit der bewussten und eindeutigen Einwilligung des Nutzers möglich.
- Für eine Anonymisierung reicht es in der Regel nicht aus, einen Hashwert aus der IP-Adresse zu bilden. Auch wenn dieser Hashwert nicht zurückgerechnet werden kann, so besteht die Möglichkeit, eine Vergleichstabelle zu errechnen, mittels derer die ursprüngliche IP-Adresse eindeutig bestimmt werden kann. Zur Wirksamkeit einer Hashwertberechnung in diesem Fall muss ein Zufallswert (sog. „Salt“) hinzugerechnet werden, der regelmäßig geändert und nicht mitgespeichert wird.
- Eine Geolokalisierung mit vollständigen IP-Adressen ist nur mit bewusster und eindeutiger Einwilligung des Spielers möglich. Liegt diese nicht vor, so muss die IP-Adresse so gekürzt werden, dass eine Personenbeziehbarkeit ausgeschlossen werden kann.
- Nach dem Ablauf der zulässigen Speicherfristen sollten die IP-Adressen automatisch gelöscht werden. Hierbei sind auch ggf. vorhandene Backups zu beachten.
- Werden personenbezogene Daten über das Internet verschickt, so sollte möglichst eine Verschlüsselung (z. B. SSL) eingesetzt werden.

9.2.27 Einbindung in Soziale Netzwerke

a) Funktionalitätsbeschreibung

Online-Spiele können in bestehende Soziale Netzwerke wie Facebook oder StudiVZ eingebunden werden. Hierbei wird ggf. auf die Struktur des Sozialen Netzwerks bzw. die darin gespeicherten Kontakte von dem Online-Spiel Zugriff genommen.

b) Relevante Normen

- § 11 ff. TMG
- §§ 3a, 4, 4a, 28 BDSG

c) Restriktionen

Auf die Kontaktinformationen innerhalb eines Sozialen Netzwerks darf nur mit Einwilligung des Spielers Zugriff genommen werden. Sollen die personenbezogenen Daten der „Kontakte“ (teilweise auch bezeichnet als „Freunde“) durch den Betreiber des Online-Spiels weiter verarbeitet werden, so sind ggf. auch die Einwilligungen der „Kontakte“ einzuholen.

Für den Spieler muss erkennbar sein, welche Daten aus seinem Profil an den Spiele-Betreiber übermittelt werden und auf welche Daten dieser dauerhaft Zugriff hat, selbst wenn der Spieler sie im Sozialen Netzwerk nachträglich ändert / ergänzt.

d) Mögliche Lösungen

- Bevor ein Online-Spiel in ein Soziales Netzwerk eingebunden wird, muss dem Spieler dargestellt werden, welche Daten dem Betreiber des Spiels übermittelt werden und auf welche er aktiv zugreifen kann. Hierbei sollten die Angaben so weit wie möglich präzisiert und keine Pauschalangabe verwendet werden.
- Dem Spieler sollte ermöglicht werden, seine an den Spiele-Betreiber übermittelten Daten frei zu wählen.
- Der Spieler muss jederzeit die Möglichkeit haben, das Spiel wieder zu entfernen und Zugriffe zu unterbinden.
- Für den Spieler muss die Firma, die das Online-Spiel anbietet, klar mit Adressangabe erkennbar sein. Es sind von dem Betreiber die entsprechenden rechtlichen Vorgaben für die Registrierung zu einem Online-Spiel etc. einzuhalten.
- Sollen Daten auch von Kontakten des Spielers verwendet werden, so müssen die Einwilligungen der betroffenen Kontakte eingeholt werden.

e) Weiterführende Literatur

- Artikel 29-Datenschutzgruppe: Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke:
  http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_de.pdf.
- Beschluss des Düsseldorfer Kreises vom 17./18. April 2008 – Datenschutzkonforme Gestaltung sozialer Netzwerke:
  http://www.bfdi.bund.de/cae/servlet/contentblob/416850/publicationFile/25166/170408DatenschutzkonformeGestaltungSozNetzwerke.pdf.

10 Datenschutz in Online-Spielen – Was sagen die Spieler?

In den vorangegangenen Kapiteln wurden unter anderem die rechtlichen Rahmenbedingungen für den Datenschutz in Online-Spielen dargelegt. Das Ziel dieses Abschnitts ist es zu untersuchen, ob Datenschutz in Online-Spielen auch den Nutzern von solchen Spielen präsent ist und welchen Wert sie ihm beimessen. Ist der „gläserne Spieler“ für die Teilnehmer von Online-Spielen ein Horror-Szenario oder begrüßen sie die Möglichkeit, persönliche Daten, wie z. B. Spielprofile, online abrufen zu können?

An den Daten über den Spieler und sein Spielverhalten haben vielerlei Gruppen Interesse. Zum einen möchten sich die Spieler untereinander mit ihren Spielerprofilen und -leistungen präsentieren, zum anderen hat die Industrie ein erhebliches Interesse an Profildaten, um Produkte optimal vermarkten zu können. Ein Beispiel dafür ist die (personalisierte) Werbung in Online-Spielen, In-Game-Advertising genannt. Zusätzlich hat eine Reihe von Herstellern und Betreibern von Online-Spielen ein Interesse an Informationen über das Geschehen auf dem PC bzw. der Spielkonsole, von wo aus das Online-Spiel gespielt wird, um den von ihnen erwünschten Einsatz ihrer Produkte sicherzustellen. Dazu kommen fragwürdige Maßnahmen wie die automatische Durchsuchung von Festplatten nach Cheat-Programmen[115], das Übertragen und Auswerten von Screenshots[116] oder DRM-Systeme[117] zum Einsatz, die zumeist nicht unerheblich in die Systeme des Spielers eingreifen. Die Verwendung solcher Maßnahmen erfolgt vornehmlich, um Raubkopien der Spiele einzuschränken und um zu verhindern, dass Spieler durch Zusatzprogramme das Spielgeschehen manipulieren. Ein Großteil dieser Aktivitäten wird im „Hintergrund“, d. h. ohne ausreichende Information des Spielers, durchgeführt und greift in dessen Privatsphäre und andere Persönlichkeitsrechte ein.

Aussagen zu dem Thema, inwiefern sich Spieler von Online-Spielen über Datenschutzprobleme im Klaren sind und welche Einstellung sie hierzu haben, sind in der Wissenschaft kaum zu finden. Zwar gibt es mittlerweile einen umfangreichen Bestand an Forschung zu Online-Spielen allgemein; das Thema Datenschutzbewusstsein wird aber nur sehr selten angesprochen. Die sozialwissenschaftlichen Arbeiten beziehen sich größtenteils auf Fragen der demographischen Zusammensetzung der Spieler und Auswirkungen von Online-Spielen,

[115] Cheat-Programme versuchen den Spielverlauf durch nicht den vom Hersteller vorgegebenen Regeln entsprechender Funktionalität zu beeinflussen.

[116] Als Screenshot bezeichnet man ein graphisches Abbild des Bildschirminhalts.

[117] Ein Beispiel hierfür das Spiel „Spore“, das aufgrund eines restriktiven DRM in die Kritik geriet. http://www.theregister.co.uk/2008/09/10/spore_drm_amazon_effect/.

etwa Suchtgefahren.[118]

Eine der wenigen Ausnahmen ist eine Studie von Clyde Holsapple und Jiming Wu[119], die untersucht haben, welche Charakteristiken Webseiten von Online-Spielen aufweisen müssen, um auf die Spieler vertrauenswürdig zu wirken. Auch wenn das Interface-Design und die wahrgenommene Qualität des Spiels selbst als Kontrollvariablen zugelassen werden, bleibt demnach das Vertrauen der Spieler in die Sicherheit der Webseite der wichtigste Prädiktor für das Gesamtvertrauen. Zu ähnlichen Ergebnissen kommt eine weitere Untersuchung[120], nach der dieses Vertrauen ein wichtiger Vorhersagefaktor für die Einstellung gegenüber Online-Spielen ist.[121]

Im Rahmen der Studie „Datenschutz in Online-Spielen" wurde eine empirische Untersuchung durchgeführt, in der Online-Spieler speziell zum Themenkomplex „Datenschutz in Online-Spielen" befragt wurden. Die Ergebnisse dieser Untersuchung werden im Folgenden dargestellt.

10.1 Der typische Online-Spieler – Demographie der Online-Spieler

Online-Spiele werden in der öffentlichen Debatte größtenteils als ein Hobby männlicher Jugendlicher wahrgenommen. Dementsprechend dreht sich die öffentliche Diskussion um Fragen des Jugendschutzes, eingeschlossen der Thematik einer möglichen Spielesucht und anderen Auswirkungen von Online- oder allgemeinen Computer-Spielen. Empirische Arbeiten zur Demographie von Spielern haben diese Stereotypen jedoch größtenteils widerlegt oder zumindest modifiziert.[122] Im Folgenden wird ein kurzer Überblick zum Stand der Forschung zu Fragen der Geschlechterverteilung, der Altersverteilung, der Spieldauer sowie des

---

[118] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018.
Ferguson, The Good, The Bad and the Ugly: A Meta-analytic Review of Positive and Negative Effects of Violent Video Games, in: Psychiatric Quarterly 78(4), 2007, S. 309-316.
Jansz / Tanis, Appeal of Playing Online First Person Shooter Games, in: Cyberpsychology & Behavior 10(1), 2007, S. 133-136.

[119] Holsapple / Wu, Building effective online game websites with knowledge-based trust, in: Information Systems Frontiers 10(1), 2008, S. 47-60.

[120] Wu / Liu, The effects of trust and enjoyment on intention to play online games, in: Journal of Electronic Commerce Research 8(2), 2007, S. 128-140.

[121] Ein direkter Einfluss des Vertrauens auf die Absicht, ein Spiel zu spielen, wurde dort nicht gefunden. Allerdings wurde in der Studie nicht zwischen kostenpflichtigen und kostenlosen Angeboten unterschieden. Zudem wurde das Vertrauen in das Spiel selber nicht als Variable aufgenommen. Es kann angenommen werden, dass kostenpflichtige Angebote ein höheres Maß an Vertrauen voraussetzen (S. 136).

[122] Vgl. Griffiths / Davies / Chappell, Breaking the Stereotype: The Case of Online Gaming, in: Cyberpsychology & Behavior 6(1), 2003, S. 81-91.
Griffiths / Davies / Chappell, Demographic Factors and Playing Variables, in: Online Computer Gaming. In: Cyberpsychology & Behavior 7(4), 2004, S. 479-487.
Yee, The Demographics, Motivations and Derived Experiences of Users of Massively-Multiuser Online Graphical Environments, in: PRESENCE: Teleoperators and Virtual Environments 15(3), 2006, S. 309-332.
Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018.

Gesundheitszustands (körperlich und seelisch) gegeben. Da sich die demographische Zusammensetzung in einigen Aspekten je nach Spielart unterscheidet, wird gegebenenfalls auf entsprechende Unterschiede hingewiesen. Die Studien zu diesen Fragestellungen wurden in der Regel über Online-Umfragen durchgeführt, die auf Webseiten, die sich an Spieler richten, verlinkt wurden. Die Studien basierten zumeist auf einer nicht repräsentativen Stichprobe. Eine Ausnahme hiervon stellt die Umfrage des Branchenverbandes ESA dar[123], die zumindest für die Haushalte, die eine Spielkonsole oder einen PC besitzen, repräsentativ ist. Die meisten Studien basieren auf Testgruppen (Samples), die hauptsächlich aus US-Amerikanern bestanden, so dass eine vollständige Übertragbarkeit der Ergebnisse auf die Situation in Deutschland fraglich ist. Ausnahmen sind Sozioland[124] (Teilnehmer aus dem deutschsprachigen Raum) und die Studie von Jansz und Tanis[125], die auf einem Sample aus Niederländern basiert.

Mehrere Studien, die speziell auf Spieler von MMORPGs zielten[126], kommen zu einem Geschlechterverhältnis von im Schnitt 83% männlich zu 17% weiblich[127]. Die Sozioland-Umfrage, die sich allgemeiner auf die Nutzung von Computerspielen bezog[128], zeigt ein ähnliches Verhältnis (87% männlich, 13% weiblich), während Spiele wie First Person Shooter[129] (FPS) praktisch ein rein männliches Publikum anziehen[130]. Zu erheblich abweichenden Ergebnissen kommt eine Umfrage des amerikanischen Branchenverbandes Entertainment Software Association[131], nach der der Frauenanteil bei 44% liegt.

---

123 ESA, Sales, Demographic and Usage Data. Essential Facts about the Computer and Video Game Industry, 2008.

124 Sozioland, Tabellenband Sozioland Games 2008, 2008.

125 Jansz / Tanis, Appeal of Playing Online First Person Shooter Games, in: Cyberpsychology & Behavior 10(1), 2007, S. 133-136.

126 Befragt wurden in diesen Studien Spieler des MMORPG „Everquest 2“, das vor „World of Warcraft“ ein Marktführer war.

127 Mittelwert berechnet aus
Griffiths / Davies / Chappell, Breaking the Stereotype: The Case of Online Gaming, in: Cyberpsychology & Behavior 6(1), 2003, S. 81-91.
Griffiths / Davies / Chappell, Demographic Factors and Playing Variables, in: Online Computer Gaming. In: Cyberpsychology & Behavior 7(4), 2004, S. 479-487.
Yee, The Demographics, Motivations and Derived Experiences of Users of Massively-Multiuser Online Graphical Environments, in: PRESENCE: Teleoperators and Virtual Environments 15(3), 2006, S. 309-332.
Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018.

128 Allerdings hat auch in dieser Befragung mindestens die Hälfte der Befragten bereits einmal ein MMORPG gespielt.

129 First Person Shooter ist ein Synonym für Ego-Shooter. Dabei handelt es sich um Computerspiele, die aus der Perspektive des Spielers bzw. der Spielfigur gespielt werden.

130 Jansz / Tanis, Appeal of Playing Online First Person Shooter Games, in: Cyberpsychology & Behavior 10(1), 2007, S. 133-136.

131 ESA, Sales, Demographic and Usage Data. Essential Facts about the Computer and Video Game Industry, 2008.

Tabelle 6: Geschlechterverteilung in Online-Spielen: Vergleich verschiedener Studien

Studie	Anteil weiblich	Anteil männlich	Zielgruppe der Befragung	Stichprobe
Yee 2006	15%	85%	MMORPG	5.547
Griffiths / Davies / Chappell 2004	19%	81%	MMORPG	540
Williams / Yee / Caplan 2008	19%	81%	MMORPG	7.000
Jansz / Tanis 2007	1%	99%	FPS	752
ESA 2008	44%	56%	Online-Spiele allgemein	1.200
Sozioland 2008	13%	87%	Computerspiele allgemein	6.659

Die Studie der ESA unterscheidet sich von den anderen erwähnten Arbeiten hauptsächlich dadurch, dass sie nicht primär auf die Spieler von MMORPGs oder FPS zielte, sondern auf Online-Spiele im Allgemeinen. Insgesamt ist festzustellen, dass die Einschätzung, Online-Spiele seien hauptsächlich ein Hobby von Männern, nur in Bezug auf MMORPGs und FPS zutrifft; wenn man das gesamte Feld der Online-Spiele betrachtet, ist ein deutlich ausgewogeneres Bild festzustellen.

Die Annahme, dass es sich bei Online-Spielern hauptsächlich um Jugendliche handelt, wird in den meisten empirischen Arbeiten klar widerlegt. Die Ausnahme hiervon bilden wiederum FPS, die ein jüngeres Publikum anzuziehen scheinen.[132] In der Studie von Jansz und Tanis lag das Durchschnittsalter bei 18 Jahren. Für MMORPG-Spieler ergibt sich über die Studien von Griffiths, Davies und Chappell[133] sowie Yee[134] und Williams, Yee und Caplan[135] ein Mittelwert von 29 Jahren. Die ESA gibt sogar ein Durchschnittsalter von 35 Jahren an.[136] Bei Griffiths, Davies und Chappell[137] und Sozioland[138] wurde das Alter per Einstufung in Altersgruppen abgefragt. Der Gipfel der Verteilung lag in diesen beiden Studien in den Altersgrup-

[132] Jansz / Tanis, Appeal of Playing Online First Person Shooter Games, in: Cyberpsychology & Behavior 10(1), 2007, S. 133-136.

[133] Griffiths / Davies / Chappell, Demographic Factors and Playing Variables, in: Online Computer Gaming. In: Cyberpsychology & Behavior 7(4), 2004, S. 479-487.

[134] Yee, The Demographics, Motivations and Derived Experiences of Users of Massively-Multiuser Online Graphical Environments, in: PRESENCE: Teleoperators and Virtual Environments 15(3), 2006, S. 309-332.

[135] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, In: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018.

[136] Allerdings auf Computerspieler insgesamt bezogen, vgl. ESA, Sales, Demographic and Usage Data. Essential Facts about the Computer and Video Game Industry, 2008, S. 2.

[137] Griffiths / Davies / Chappell, Breaking the Stereotype: The Case of Online Gaming, in: Cyberpsychology & Behavior 6(1), 2003, S. 81-91.

[138] Sozioland, Tabellenband Sozioland Games 2008, 2008.

pen 21-30 bzw. 20-24. Auffallend ist, dass Spielerinnen im Schnitt älter sind.[139]

Eine weitere oft behandelte Frage ist die nach der Spieldauer und den Risiken für eine Spielsucht. Als Stereotyp gilt der jugendliche Vielspieler. Auch diese Stereotypen werden durch Studien widerlegt; ältere Spieler spielen zumindest bei MMORPGs länger als jüngere. Zudem spielten im beobachteten Sample von MMORPG-Spielern Frauen länger als Männer.[140] Die durchschnittliche Spielzeit für erwachsene US-Bürger beträgt 7,5 Stunden pro Woche.[141] Interessanterweise zeigen sich hierbei starke Verdrängungseffekte gegenüber dem Fernsehkonsum; im Schnitt sahen die befragten Spieler pro Woche 10 Stunden weniger fern als die Gesamtbevölkerung.[142]

Fragen zum Gesundheitszustand wurden in Studien am häufigsten in Zusammenhang mit dem Suchtpotential gestellt. Allgemeine Fragen zur Gesundheit von Online-Spielern wurden dagegen explizit in einer Studie von Williams, Yee und Caplan gestellt.[143] Die Ergebnisse haben gezeigt, dass Spieler von MMORPGs im Vergleich zur Gesamtbevölkerung körperlich besser in Form waren[144], seelisch aber in schlechterer Verfassung. Indikator hierfür war, ob bei den Teilnehmern jemals eine Depression diagnostiziert wurde und ob Drogen- oder Medikamentenmissbrauch stattgefunden hat. Die Häufigkeit von Depressionen war gegenüber der Gesamtbevölkerung deutlich größer, die Häufigkeit von Substanzmissbrauch leicht erhöht. Allerdings zeigte sich beim dritten Indikator für die seelische Gesundheit, der Häufigkeit von Angststörungen, eine geringere Häufigkeit als in der Gesamtbevölkerung.

Ein weiterer wichtiger Komplex im Bereich der seelischen Gesundheit ist die Frage nach einem eventuell erhöhten Aggressionsniveau bei Spielern. Hierbei ist jedoch in der Forschung kein Konsens zu beobachten.

Die verschiedenen Studien und Untersuchungen konnten somit das Vorurteil, dass es sich bei Online-Spielern fast ausnahmslos um männliche jugendliche Vielspieler handelt, nicht bestätigen. Das Stereotyp des jugendlichen männlichen Vielspielers ist genau das: ein Stereotyp. „Die“ Online-Spieler insgesamt sind älter und zu einem deutlich höheren Anteil weiblich, als vermutet wird. Einige Genres wie FPS scheinen das Stereotyp zwar zu bestätigen; allerdings sind diese nicht repräsentativ für die Gesamtheit der Online-Spiele: FPS machten

---

[139] Yee, The Demographics, Motivations and Derived Experiences of Users of Massively-Multiuser Online Graphical Environments, in: PRESENCE: Teleoperators and Virtual Environments 15(3), 2006, S. 309-332.

[140] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018, S. 1002.

[141] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018, S. 1002.

[142] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018, S.1004.

[143] Williams / Yee / Caplan, Who plays, how much, and why? Debunking the stereotypical gamer profile, in: Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018, S. 1005.

[144] Basierend auf dem Body Mass Index (BMI) und der Häufigkeit sportlicher Betätigung.

2007 in den USA nur ca. 12% der verkauften Spiele aus.[145]

10.2 Empirische Untersuchung – Eine Befragung

Das Ziel der Befragung war es zu untersuchen, ob den Spielern von Online-Spielen die Risiken, die sich aus unangemessenem Umgang mit ihren persönlichen Daten ergeben, bewusst sind und wie wichtig ihnen das Datenschutzniveau in Online-Spielen ist.

Nachfolgend werden die Durchführung und die Methodik der Befragung, sowie der Aufbau des Fragebogens dargestellt. Daran anschließend wird noch auf Besonderheiten bei der Auswertung bzw. Aufbreitung des Datenmaterials eingegangen, bevor im darauf folgenden Kapitel die Ergebnisse der Befragung vorgestellt werden.

10.2.1 Durchführung

Die Befragung wurde mittels eines Fragebogens im Web online durchgeführt.[146] Dabei konnten die Teilnehmer sich zum Themenkomplex „Datenschutz in Online-Spielen“ äußern.

Die Umfrage startete am 7. August 2008 mit dem Freischalten des Online-Fragebogens auf dem Server des ULD. Durch eine Pressemitteilung wurde die Befragung der Öffentlichkeit vorgestellt. Die Pressemitteilung wurde von vielen Online-Medien aufgegriffen, die dann über das Projekt DOS und die Befragung berichteten. In den meisten Berichten der Online-Medien wurde ein Link[147] zu der Befragung veröffentlicht, so dass die Leser mit einem Klick zu der Befragung wechseln und teilnehmen konnten. Ein sehr leserstarkes Online-Medium, das über die Befragung und das Projekt „DOS“ berichtete, war „heise online“[148].

Die Befragung sollte ursprünglich bis zum Ende des Jahres 2008 online sein. Zu diesem Zeitpunkt wurde klar, dass die Berichterstattung über die Befragung auf „heise online“ und in anderen Online-Medien vorrangig die Leser über 18 Jahre angesprochen hat. Daher wurde zusätzlich in mehreren Online-Spiele-Foren aktiv auf die Befragung hingewiesen, um auch jüngere Online-Spieler zur Teilnahme an der Befragung zu bewegen. Schließlich blieb die Befragung bis zum 10. Mai 2009 online und hatte insgesamt 1217 Teilnehmer. Die Befragung war ununterbrochen aktiv, und Besucher der Webseite konnte ohne Einschränkungen an der Umfrage teilnehmen.

---

[145] ESA, Sales, Demographic and Usage Data. Essential Facts about the Computer and Video Game Industry, 2008, S. 5.

[146] Der Fragebogen befindet sich im Anhang.

[147] Querverweis im WWW von einer Webseite zu einer anderen Webseite.

[148] www.heise.de; Teil des Heise Zeitschriften Verlags http://www.heise.de/newsticker/Maengel-beim-Datenschutz-in-Online-Spielen-beklagt--/meldung/113942.

10.2.2 Methodik

Quantitative Umfragen sind ein bewährtes Mittel der Sozialforschung; in den letzten Jahren sind aufgrund des technischen Fortschritts insbesondere Web-Umfragen beliebter geworden. Eine solche wurde im Rahmen des Vorhabens DOS durchgeführt. Befragungen über das Web haben jedoch einige methodische Besonderheiten, deren wichtigsten Punkte im Folgenden kurz vorgestellt werden.

Ein entscheidender Vorteil von Befragungen über das Web sind die niedrigen Kosten, da keine Interviewer nötig sind, die Daten automatisch kodiert vorliegen und nicht mehr von Hand erfasst werden müssen. Allerdings gibt es auch Nachteile, die statistische Inferenzen, also aus der Stichprobe abgeleitete Aussagen über eine Grundgesamtheit, in den meisten Fällen unmöglich machen,[149] Dies betrifft die Punkte sogenannter „Coverage Errors", „Sampling Errors" und besonders die Selbst-Selektion.[150] Zusätzlich ergeben sich Ungenauigkeiten durch das mögliche Mehrfach-Ausfüllen von Fragebögen durch einzelne Teilnehmer.

„Coverage Errors" entstehen, wenn die Grundgesamtheit, aus der die Stichprobe gezogen wird, nicht klar definiert ist oder nicht der Grundgesamtheit, über die eine Aussage getroffen werden soll, entspricht. „Sampling Errors" entstehen, wenn nicht jedes Mitglied der Grundgesamtheit eine gleiche (oder zumindest bezifferbare und dann per Gewichtung ausgleichbare) Wahrscheinlichkeit hat, in die Stichprobe aufgenommen zu werden. Da für Web-Umfragen in der Regel weder eine vollständige Liste der möglichen Teilnehmer vorliegt, noch eine echte Zufallsauswahl vorgenommen werden kann, werden häufig selbst-selektierte Samples verwendet,[151] bei denen die Umfrage auf Portalen, populären Webseiten oder speziellen Befragungswebseiten beworben wird. Hier nehmen in der Regel nur sehr wenige der Personen, die von dem Aufruf erreicht wurden, an der Umfrage teil.[152] Zudem ist es wahrscheinlich, dass sich die Teilnehmer systematisch von den Nicht-Teilnehmern unterscheiden,[153] insbesondere dadurch, dass sie ausgeprägtere Meinungen zum Thema der Umfrage haben.

Zusätzlich ist es möglich, dass einzelne Teilnehmer mehrmals an der Umfrage teilnehmen

---

[149] Schnell / Hill / Esser, Methoden der empirischen Sozialforschung. 7. völlig überarbeitete und erweiterte Auflage. München: Oldenburg, 2005, S. 377.

[150] Couper / Coutts, Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in: Diekmann, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, S. 217-243, S. 219-222.

[151] Couper / Coutts, Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in: Diekmann, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, S. 217-243, S. 229; s.a. Schnell / Hill / Esser, Methoden der empirischen Sozialforschung. 7. völlig überarbeitete und erweiterte Auflage. München: Oldenburg, 2005, S. 297f.

[152] In der Regel 0,5% oder weniger, siehe Couper / Coutts, Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in: Diekmann, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, S. 217-243, S. 229.

[153] Couper / Coutts, Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in: Diekmann, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, S. 217-243, S. 230f.

und so die Ergebnisse verfälschen.[154] Eine Möglichkeit, dies einzuschränken, bestünde darin, IP-Adressen der Teilnehmer für einen bestimmten Zeitraum zu speichern, um zumindest direkt hintereinander erfolgendes mehrfaches Ausfüllen zu verhindern. Bei der Durchführung dieser Web-Befragung wurde darauf verzichtet, IP-Adressen zu speichern, um die Anonymität der Teilnehmer sicherzustellen. Mehrfaches Ausfüllen durch einzelne Teilnehmer konnte somit nicht ausgeschlossen werden.

Die Stichprobe ist aus den oben angegebenen Gründen nicht repräsentativ. Aussagen über die Grundgesamtheit der Online-Spieler lassen sich aus den Ergebnissen der Befragung daher nicht ableiten. Die Kosten für eine repräsentative Umfrage wären unverhältnismäßig hoch und im Rahmen dieses Vorhabens nicht notwendig gewesen. Es ging bei der Erarbeitung dieser Studie lediglich darum, Trendaussagen zum Themenkomplex „Datenschutz in Online-Spielen“ zu ermitteln. Auf Faktoren, die verschiedene Bevölkerungsgruppen widerspiegeln, wurde deshalb, mit Ausnahme des Alters, nicht geachtet. Die Teilnahme an der Befragung war nicht beschränkt, es konnten alle Personen an der Umfrage teilnehmen. Die Umfrage richtete sich an Spieler von Online-Spielen.

10.2.3 Fragebogen

Der Fragebogen enthielt insgesamt 15 Fragen zu Datenschutz und Online-Spielen.[155] Der Fragebogen ließ sich dabei in die folgenden thematischen Blöcke unterteilen:

- Teilnehmer an der Umfrage
  In diesem Bereich wurde die Zugehörigkeit zu Alterklassen (Frage 1) und Ausstattung mit Spiele-Hardware (Frage 2) abgefragt.
- Spielverhalten
  Der Frageblock (Fragen 3 bis 6) befasste sich mit dem Spielverhalten und der Nutzung von Online-Spielen. Hier wurde unter anderem erhoben, mit welchen Geräten bzw. Systemen online gespielt wird (Frage 3) und welche Spiele dabei verwendet werden (Frage 6).
- Datenschutzaffinität
  Mit dem letzten Fragenblock (Fragen 7 bis 14) wurde die Einstellung der Online-Spieler zum Thema Datenschutz abgefragt. Dabei wurden sowohl sehr detaillierte Fragen als auch verallgemeinerte Meinungen zu dem Thema abgefragt.
- Anmerkungen
  Zum Schluss des Fragebogens (Frage 15) hatten die Teilnehmer der Befragung die

[154] Couper / Coutts, Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in: Diekmann, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, S. 217-243, S. 229.

[155] Der Fragebogen befindet sich im Anhang.

Möglichkeit, Anmerkungen oder Hinweise zum Thema Datenschutz in Online-Spielen abzugeben.

Im Rahmen dieses Fragebogens wurden sowohl offene als auch geschlossene Fragen verwendet. Insbesondere die offenen Fragen sollten dazu dienen, Hinweise auf Datenschutzproblematiken in Online-Spielen zu bekommen und diese Informationen in die anderen Teile dieses Vorhabens einfließen zu lassen.

Vor dem eigentlichen Start der Online-Befragung wurden die Teilnehmer mit einem kurzen Einführungstext begrüßt, der neben der geschätzten Dauer auch die thematische Ausrichtung der Befragung enthielt. Es wurde darauf hingewiesen, dass die Befragung anonym erfolgt. Für etwaige Rückfragen wurden Kontaktdaten angegeben.

Der Fragebogen wurde technisch so angelegt, dass auf einer Webseite alle Fragen aufgelistet waren. Es wurde keine technische Bedingung implementiert, die eine Beantwortung aller Fragen vom Teilnehmer forderte. Bei den geschlossenen Fragen gab es Fragen, bei denen nur eine Antwort zulässig war (dies wurde technisch entsprechend begrenzt.), bei anderen waren Mehrfachantworten zulässig. Der Fragebogen musste nach Beantwortung der Fragen durch den Teilnehmer mit einem Klick auf den Button „Umfrage senden“ abgeschlossen werden. Die Einträge der Teilnehmer wurden daraufhin in einer Datenbank abgelegt. Die Antworten von Fragebögen, bei denen dieser abschließende Schritt durch den Teilnehmer nicht durchgeführt wurde, wurden nicht in die Datenbank geschrieben. Diese Daten standen somit nicht für die Auswertung zu Verfügung, sondern wurden automatisch verworfen.

10.2.4 Besonderheiten bei der Auswertung

Während der Befragung im Web wurden die Antworten von 1217 Fragebögen in der Datenbank abgelegt.

Bei insgesamt vier Fragebögen wurde keine einzige Frage beantwortet. Es ist davon auszugehen, dass es sich um eine Fehlbedienung eines Teilnehmers handelte oder kein wirkliches Interesse zur Teilnahme an der Befragung vorlag. Diese Datensätze wurden für die Auswertungen nicht herangezogen. Für die Auswertung standen somit 1213 beantwortete Fragebögen bzw. Datensätze zur Verfügung.

Bei den Fragen nach den Geräten, die im Haushalt vorhanden sind (Frage 2), welche davon in den letzten drei Monaten online genutzt wurden (Frage 3) und welcher Online-Zugang für die Online-Spiele genutzt wird (Frage 5), waren Mehrfachantworten zulässig. Dabei brachte ein Haken des Teilnehmers ein „Ja“ zum Ausdruck: „Ja, das Gerät ist im Haushalt vorhanden“ oder „Es wurde in den letzten drei Monaten online genutzt“. Bei der weiteren Auswertung der Antworten wurde davon ausgegangen, dass ein nicht gesetzter Haken ein „Nein“ ausdrückt. Die Kategorie „keine Antwort“ gab es bei diesen drei Fragen damit nicht. Dieses Vorgehen diente zur Analyse der Daten. Statistische Aussagen sind damit nur hinsichtlich der „Ja“-Antwort zulässig.

Die Frage „Wie lange spielen Sie durchschnittlich pro Woche online?“ (Frage 4) wurde von

den allermeisten Teilnehmern dazu genutzt, eindeutige Zahlenwerte anzugeben. Bei Antworten, die eine Spanne angaben (z. B. „2-10“ Stunden), wurde der Mittelwert der Antwort (bei diesem Beispiel „6“ Stunden) für die weiteren Auswertungen herangezogen. Antworten in Textform, die nicht eindeutig interpretiert werden konnten, wurden entsprechend kodiert und den „Missing Values“[156] zugeordnet.

Im Rahmen des Fragebogens wurden die Teilnehmer gebeten anzugeben, welche Online-Spiele von ihnen am meisten gespielt werden. Diese Spiele sollten in Form einer „Top 5“-Liste in Freitext-Felder eingegeben werden. Bei der Kodierung[157] der Freitextantworten wurden Spiele und ihre verschiedenen Versionen bzw. Abwandlungen zu einer Gruppe zusammengefasst. Eine Antwortgruppe wurde gebildet, wenn mehr als 20 Nennungen über die Gesamt-„Top 5“-Frage mit seinen fünf Antwortfeldern zu verzeichnen waren. Die folgenden Spiele und deren verschiedenen Versionen und Abwandlungen wurden in eigenen Gruppen zusammengefasst: Age of Conan (Eidos Interactive), Battlefield (Electronic Arts GmbH), Brettspielwelt (Brettspielwelt GmbH), Call of Duty (Activision), Counter-Strike (Electronic Arts GmbH), Diablo (Vivendi Games / Blizzard Entertainment), EVE Online (Atari), Everquest (Sony Online Entertainment), Gears of War (Microsoft / Epic Games), Grand Theft Auto (Rockstar Games), Guild Wars (NCsoft Europe), Halo (Microsoft / Bungie), Herr der Ringe Online (codemasters online gaming), Mario Kart (Nintendo), Poker (diverse Anbieter von Online-Poker-Spielen), Quake (Activision / GT Interactive), Team Fortress (Electronic Arts GmbH), TrackMania (Nadeo), Unreal Tournament (GT Interactive / Infogrames / Epic Games), Warhammer (Electronic Arts GmbH / Games Workshop) und World of Warcraft (Vivendi Games / Blizzard Entertainment). Alle anderen Antworten wurden unter „diverse Spiele“ subsumiert.

Im Zusammenhang mit den Fragen zur Datenschutzaffinität wurde gefragt, ob es Datenschutzgründe gibt, ein Online-Spiel nicht zu nutzen, und wenn ja, welche Gründe dies sind. Die Datenschutzgründe für eine Nichtnutzung eines Online-Spiels konnten als Freitext angegeben werden. Die verschiedenen Antworten wurden gesichtet und daraufhin sieben Obergruppen gebildet, denen die einzelnen Antworten manuell zugeordnet wurden. Für die Zuordnung wurden die folgenden Gruppen identifiziert: Weitergabe von Daten, Werbung, Datenerhebung, Profiling, Spionage, Datenschutz und sonstige Gründe. Wer in Zusammenhang mit dieser Frage Gründe für eine Nichtnutzung angegeben hat, wurde automatisch der Gruppe zugeordnet, die Gründe für eine Nichtnutzung von Online-Spielen kennt. Dies war in insgesamt vierzehn Datensätzen von Bedeutung: In drei Datensätzen waren Gründe angegeben und gleichzeitig „Es gibt keine Gründe“ ausgewählt; in elf Datensätzen waren die vorgelagerte Auswahlfrage („Es gibt keine Gründe“ / „Gründe für mich wären …“) nicht beantwortet. In all diesen Fällen wurden die Antworten der Gruppe „Gründe für mich wären …“

[156] Der Begriff „Missing Value“ steht in der Statistik für einen fehlenden Wert. Die „Missing Values“ wurden nur bei der jeweiligen Auswertung nicht mit einbezogen. Datensätze mit einem oder mehreren „Missing Values“ wurden aber nicht generell aus der Stichprobe entfernt.

[157] In der Statistik verwendeter Begriff steht für die Zuordnung von Antworten zu Antwortgruppen.

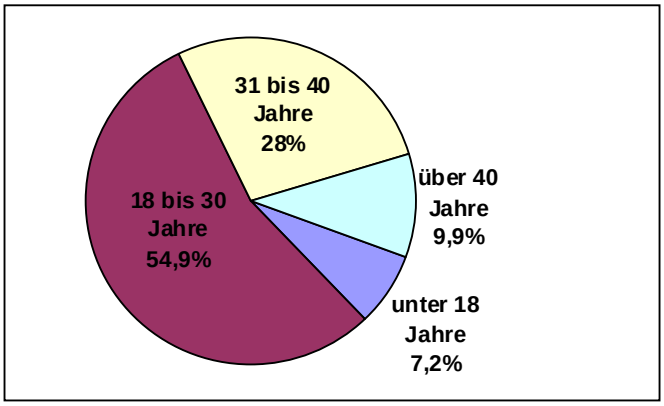
zugeordnet.

10.3 Ergebnisse und Interpretation[158]

10.3.1 Teilnehmer an der Umfrage

Bei der Altersstruktur dieser Befragung nimmt die Gruppe der 18- bis 30-Jährigen mit fast 55% die größte Gruppe ein, gefolgt von den 31- bis 40-Jährigen mit 28%. (Siehe Abbildung 4.)

Abbildung 4: Altersstruktur der Teilnehmer der Befragung

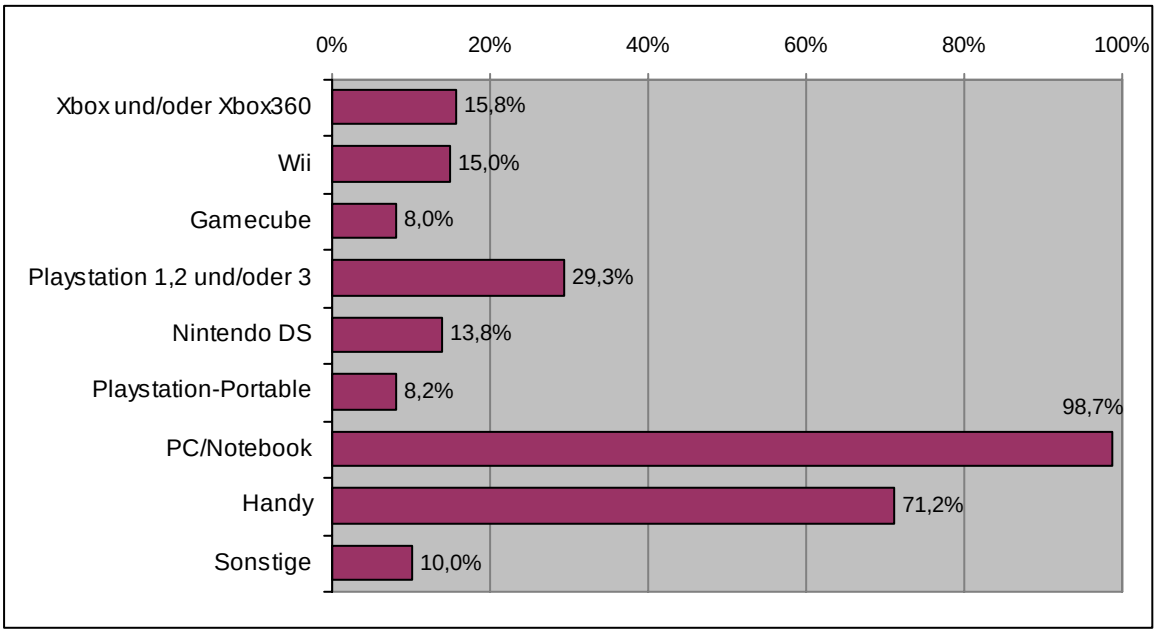


In den Haushalten der Teilnehmer, die an der Online-Befragung teilgenommen haben, sind die verschiedenen Geräte in unterschiedlicher Häufigkeit vorhanden: Erwartungsgemäß sind die meisten der Teilnehmer bzw. deren Haushalt mit PC/Notebook (98,4%) und Handy (71%) ausgestattet. Bei den Spielkonsolen ergibt sich folgendes Bild: Bei den Befragten sind 29,3% mit mindestens einer der drei Generationen der PlayStation[159], 15,8% mit Xbox und/oder Xbox 360 und 15% mit der Wii ausgestattet. (Siehe Abbildung 5.)

[158] Die Auswertung befindet sich im Anhang.

[159] Hersteller der PlayStation: Sony; Hersteller von Xbox und Xbox 360: Microsoft; Hersteller der Wii: Nintendo.

Abbildung 5: Geräte, die in den Haushalten der Befragten vorhanden sind



Als Zwischenfazit kann man zusammenfassen, dass die Gruppe der Unter-Achtzehnjährigen, die vermutlich einen nicht unbedeutenden Anteil der Online-Spieler stellt, nur zu einem kleinen Teil bei dieser Befragung vertreten ist. Zu erklären ist dieses vermutlich damit, dass sich Jugendliche nur zu einem geringen Teil für die Teilnahme an Umfragen begeistern bzw. nicht auf für diese Gruppe relevanten Kanälen angesprochen wurden.

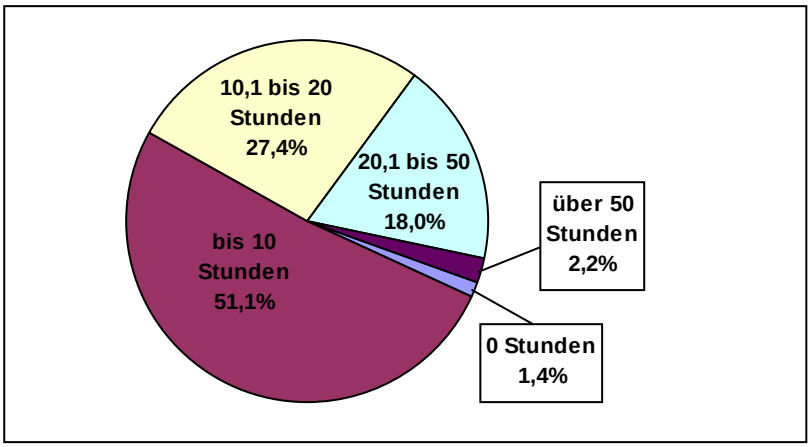
10.3.2 Spielerverhalten

Die Teilnehmer der Befragung wurden im Rahmen des Fragebogens gebeten anzugeben, wie lange sie durchschnittlich in der Woche online spielen. Die Datenanalyse ergab einen Mittelwert von 15,2 Stunden.

Im Rahmen der Auswertung wurden verschiedene Klassen von Zeiten, die die Befragten mit Onlinespielen verbringen, gebildet. Die Klassen wurden subjektiv nach grober Inaugenscheinnahme der Daten gebildet.

Es zeigt sich, dass etwas mehr als die Hälfte der an der an der Umfrage Teilnehmenden bis zu 10 Stunden pro Woche online spielen. Ein weiteres Viertel (27,4%) der Befragten spielt mehr als 10 Stunden, aber maximal 20 Stunden online pro Woche. (Siehe Abbildung 6.)

Abbildung 6: Durchschnittliche Zeit für die Beschäftigung mit Online-Spielen pro Woche



Der überwiegende Teil derjenigen, die an der Befragung teilgenommen haben, spielt bis zu 10 Stunden pro Woche Online-Spiele. Dieses ergibt bei einer angenommenen Gleichverteilung 1,4 Stunden pro Tag. Wird diesem Wert der durchschnittliche Fernsehkonsum von ca. 3,5 Stunden pro Tag[160] und einer durchschnittlichen Nutzung des Internets von 58 Minuten pro Tag[161] entgegengehalten, so spielen die meisten der Befragten Online-Spiele nicht in einem sehr übermäßigen Maße. Intensivspieler, die einen Großteil ihrer Zeit auf Online-Spiele verwenden, sind somit nur in geringem Maße an dieser Umfrage beteiligt.

In den Haushalten der Befragten sind vielfältige Geräte oder Systeme vorhanden; nicht alle davon werden für Online-Spiele genutzt.

Es ist dabei zu beobachten, dass der PC bzw. das Notebook in fast allen Haushalten der Teilnehmer dieser Umfrage vorhanden ist und zumeist online genutzt wird. Eine besonders hohe Diskrepanz bei der Online-Nutzung ist bei den Handys zu beobachten. Diese sind zwar bei 71,2% der Befragten im Haushalt vorhanden, werden aber nur in 21,6% der Fälle online genutzt. Es ist zu vermuten, dass dieses mit den hohen Kosten für mobile Online-Verbindungen zu tun hat. Die Diskrepanz bei den PlayStation-Geräten (in 29,3% Haushalten vorhanden, aber nur zu 7,3% in den letzten drei Monaten online genutzt.) ist zum Teil damit zu erklären, dass die PlayStation 1 keine Online-Funktionalität anbietet. (Siehe Tabelle 7, siehe Abbildung 7.)

[160] Fernsehkonsum für das Jahr 2004 unter http://de.wikipedia.org/wiki/Fernsehen.

[161] Durchschnittliche Nutzung des Internets in Minuten pro Tag für das Jahr 2008 unter http://de.statista.com/statistik/daten/studie/1388/umfrage/taegliche-nutzung-des-internets-in-minuten/.

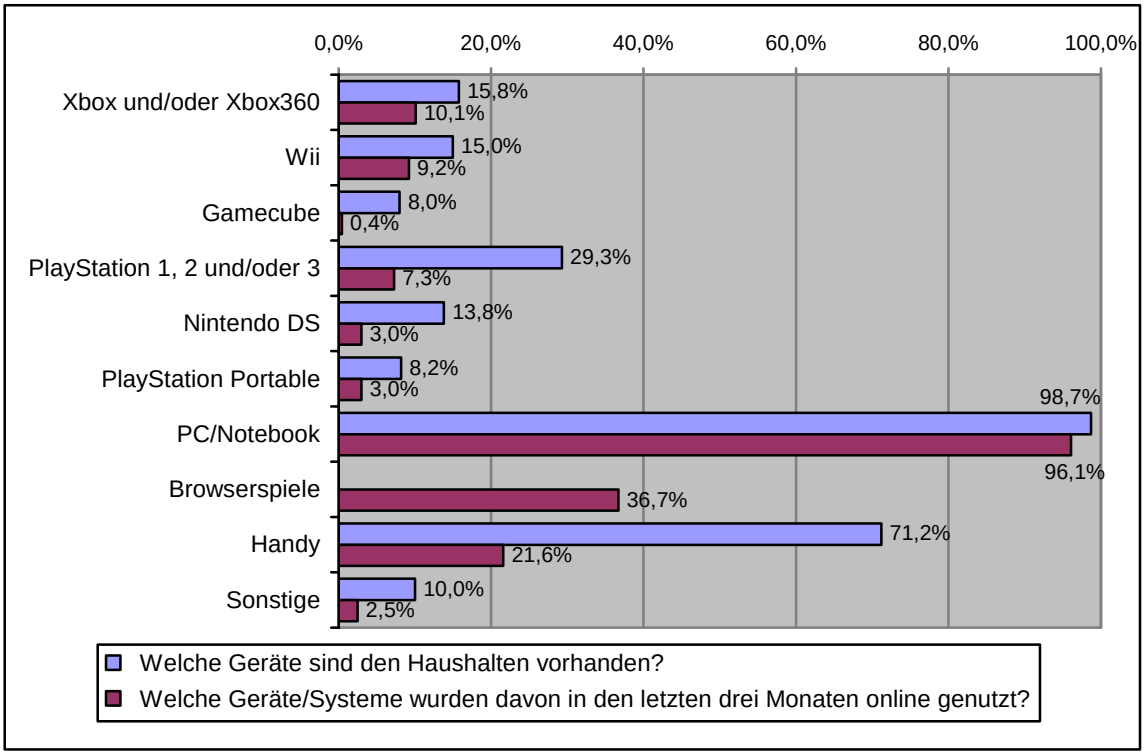
Tabelle 7: Geräte, die in den Haushalten vorhanden sind und in den letzten drei Monaten online genutzt wurden

	Welche Geräte sind in den Haushalten vorhanden?		**Welche Geräte/Systeme wurden davon in den letzten drei Monaten online genutzt?**	
Xbox	9,4%	15,8%*	1,1%	10,1%*
Xbox 360	11,4%		9,4%	
Wii	15,0%		9,2%	
Gamecube	8,0%		0,4%	
PlayStation 1	10,5%	29,3%*	- nicht online nutzbar -	
PlayStation 2	19,0%		1,7%	7,3%*
PlayStation 3	7,2%		6,0%	
Nintendo DS	13,8%		3,0%	
PlayStation Portable	8,2%		3,0%	
PC/Notebook	98,7%		96,1%	
Browserspiele/ Java-Spiele	- werden auf beliebigen Java-fähigen Endgeräten gespielt -[162]		36,7%	
Handy	71,2%		21,6%	
Sonstige	10,0%		2,5%	

* Aggregierte Werte. Der Teilnehmer der Umfrage hat mindestens eines oder mehrere der Geräte in seinem Haushalt bzw. online in den letzten drei Monaten genutzt.

[162] Für Browserspiele/Java-Spiele gibt es keine speziellen Spielekonsolen. Diese können auf beliebigen Java-fähigen Endgeräten wie z. B. Handy oder PC/Notebook gespielt werden.

Abbildung 7: Geräte, die in den Haushalten vorhanden sind und in den letzten drei Monaten online genutzt wurden



Der größte Teil der Befragten nutzt für Spiele einen DSL-Anschluss (96,2%) als Online-Zugang. Weit dahinter liegt die Mobilfunktechnologie mit 6,3%. Alle anderen Möglichkeiten für den Online-Zugang spielen mit weniger als 2,5% keine bedeutende Rolle.

Im Verlauf des Fragebogens wurden die Teilnehmer an der Befragung gebeten, die Online-Spiele anzugeben, die sie am meisten spielen. Die Antworten wurden in Form einer „Top 5"-Liste abgefragt. Die Analyse ergab dabei, dass die Teilnehmer der Befragung mit 15,8% das Online-Spiel World of Warcraft und seine diversen Abwandlungen bzw. Versionen angegeben haben. Dahinter folgten Counter-Strike (6,1%), Battlefield (5,1%) und Call of Duty (4,8%) jeweils inklusive der diversen Abwandlungen und Versionen. Alle anderen angegeben Online-Spiele sind weit abgeschlagen und haben 2,5% oder weniger Nennungen. Auf die meisten Online-Spiele entfielen dabei weniger als 1% der Nennungen als „Top 5"-Online-Spiel.

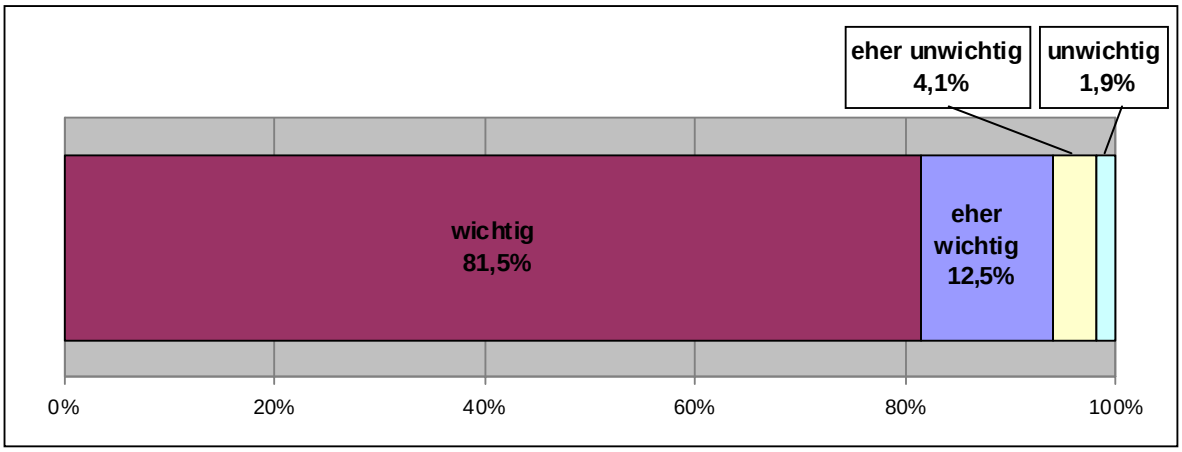
10.3.3 Datenschutzaffinität

In dem dritten Frageblock, den die Befragten beantworten konnten, ging es um Fragen und das Meinungsbild zum Thema Datenschutz in Online-Spielen.

Bei der Frage, wie vertraulich Publisher/Betreiber von Online-Spielen mit persönlichen Daten ihrer Spieler umgehen sollten, konnte man feststellen, dass diese Thematik für die meisten Befragten sehr bedeutsam ist. Mehr als 80% der Befragten, die diese Frage beantwortet

haben, gaben an, dass es ihnen wichtig ist, dass Publisher/Betreiber von Online-Spielen vertraulich mit den persönlichen Daten der Spieler umgehen. Als unwichtig ordneten es nur 1,9% der Befragten ein. (Siehe Abbildung 8.)

Abbildung 8: Wie wichtig ist der vertrauliche Umgang mit persönlichen Daten durch die Anbieter von Online-Spielen?



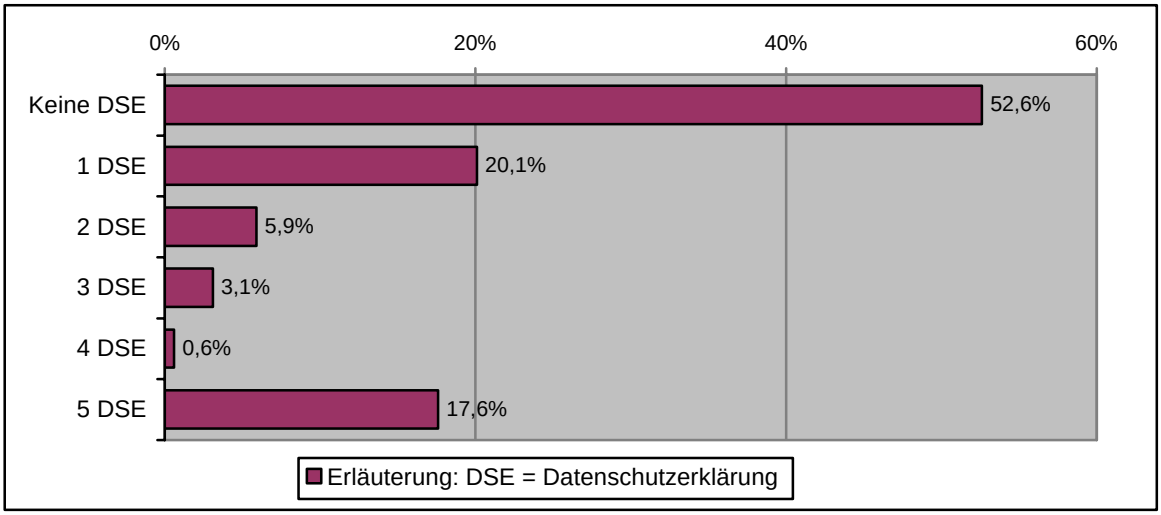
Im vorangegangenen Abschnitt wurde davon berichtet, welche Online-Spiele die Befragten am häufigsten spielen. Die Teilnehmer an der Befragung wurden ebenfalls befragt, wie viele Datenschutzerklärungen sie von den am häufigsten gespielten Online-Spielen (persönliche „Top 5“-Online-Spiele) gelesen haben.

Es zeigte sich, dass etwa die Hälfte keine einzige Datenschutzerklärung der eigenen „Top 5“-Online-Spiele gelesen hat. Etwa ein Fünftel der Befragten hat zumindest eine Datenschutzerklärung und ca. 17% haben alle Datenschutzerklärungen gelesen. (Siehe Abbildung 9.)

Obwohl die meisten der Befragten ihre „Top 5“-Online-Spiele vermutlich regelmäßig spielen, gibt es anscheinend nur eine geringe Motivation, die Datenschutzerklärungen zu lesen. Dies ist vor dem Hintergrund verwunderlich, dass die Betreiber von Online-Spielen den Umgang mit den Kundendaten größtenteils in ihren Datenschutzerklärungen regeln und diese Thematik für die Befragten sehr bedeutsam ist, wie eine der vorangegangenen Auswertungen gezeigt hat. Zu erklären ist das geringe Interesse an den Datenschutzerklärungen vermutlich damit, dass sie zumeist sehr lang, schwer verständlich und unübersichtlich gestaltet sind. Vielleicht besteht auch ein Vertrauen der Spieler darin, „dass schon nichts passieren wird“, oder sie glauben sich geschützt von deutschen Gesetzen, wie dies in anderen Lebensbereichen häufig funktioniert. Oder sie machen sich im Moment des Spielens etwaige Risiken für ihre Privatsphäre nicht bewusst, zumal die meisten Datenschutzerklärungen ihnen keine

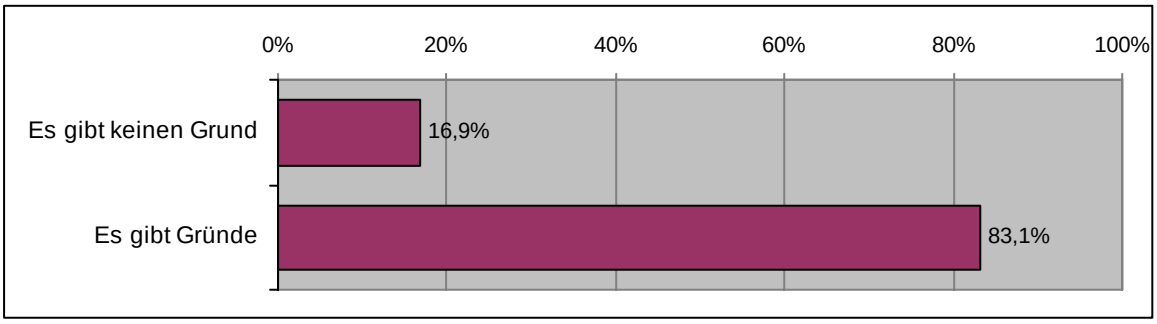
oder wenig Gestaltungsspielraum lassen.[163]

Abbildung 9: Anzahl der Datenschutzerklärungen (DSE), die von den Befragten gelesen wurden



Eine der daran anschließenden Fragen beschäftigte sich damit, ob es Gründe aus dem Bereich Datenschutz gibt, bei der die Befragten auf die Nutzung eines Online-Spiels verzichten würden. Für nur 16,9% der Befragten, die diese Frage beantwortet haben, gibt es keine Gründe, ein Online-Spiel nicht zu nutzen. Bei den Verbleibenden 83,1% gibt es Gründe im Bereich Datenschutz, ein Online-Spiel nicht zu nutzen. (Siehe Abbildung 10.)

Abbildung 10: Gibt es Datenschutzgründe, ein Online-Spiel nicht zu nutzen?



Die Befragten hatten dabei die Möglichkeit, Gründe in einem Freitextfeld zu nennen. Die „Weitergabe von Daten“ (im weitesten Sinne) wurde dabei von 57,4% der Befragten genannt,

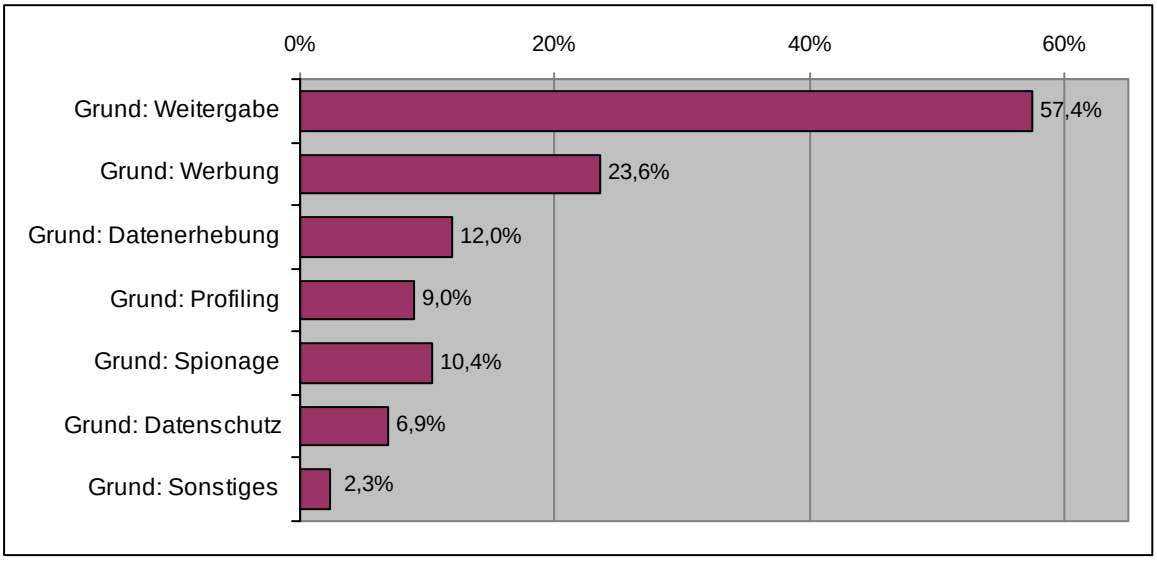
[163] Bekannt als „Privacy Paradoxon“, siehe dazu:
Spiekermann / Grossklags / Berendt, E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce, 2001, S. 28-47
Pötzsch, Privacy Awareness – A Means to Solve the Privacy Paradox?, in: The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Vol. 298, Springer 2009, S. 226-236.

die diese Frage beantwortet haben. Die Gründe „Werbung“ und „Datenerhebung“ waren mit 23,6% bzw. 12,0% weit dahintergeblieben. (Siehe Abbildung 11.)

Die Nennungen in dem Freitextfeld wurden dabei thematisch wie folgt gebündelt:

- Die Kategorie „Weitergabe“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit der Weitergabe oder dem Verkauf von Daten an Dritte und die Veröffentlichung von Daten.
- Die Kategorie „Werbung“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit Werbung, Vermarktung, In-Game-Advertising oder Spam.
- Die Kategorie „Datenerhebung“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit der Erhebung von Daten, die für das Spiel nicht notwendig sind, Registrierung mit einer Vielzahl von persönlichen Daten und die Speicherung von Chat-Protokollen.
- Die Kategorie „Profiling“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit der Auswertung von Spielerdaten und dem Spielverhalten, Bildung von Spieler-Profilen/Kunden-Profilen, Auswertung von Chatprotokollen oder anderen Online-Aktivitäten.
- Die Kategorie „Spionage“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit dem „Ausspionieren“ des Spieler PCs, Spiele bzw. eingesetzte Anti-Cheat-Programme, die im Hintergrund umfassende Analysen auf dem PC des Spielers ausführen.
- Die Kategorie „Datenschutz“ umfasst im Wesentlichen alle Nennungen im Zusammenhang mit weiteren Datenschutzthemen, die nicht in den vorherigen Kategorien enthalten sind.
- Die Kategorie „Sonstiges“ umfasst alle sonstigen vorher nicht genannten Gründe.

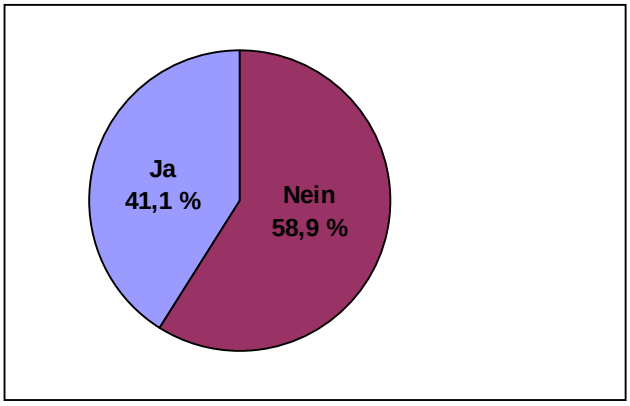
Abbildung 11: Datenschutzgründe, ein Online-Spiel nicht zu nutzen



Die hohe Anzahl an Nennungen im Bereich „Weitergabe“ hängen vermutlich mit den Datenschutzskandalen in diesem Bereich zusammen, über die in der Zeit der Erhebung häufiger von den Medien berichtet wurde, wie zum Beispiel die illegale Weitergabe von Kontodaten[164].

Mit den persönlichen Erfahrungen der Teilnehmer zu Datenschutz in Online-Spielen befasste sich die daran anschließende Frage. Die Auswertung ergab, dass 41,1% der Befragten schon einmal das Thema Datenschutz im Zusammenhang mit Online-Spielen aufgefallen ist. Bei der Beantwortung war es egal, ob der Spieler eigene Erfahrungen mit dem Thema gemacht hat oder z. B. Berichte darüber in Internet-Foren/Zeitschriften wahrgenommen hat. 58,9% der Befragten gaben an, dass ihnen das Thema Datenschutz in Zusammenhang mit Online-Spielen noch nicht aufgefallen war. (Siehe Abbildung 12.)

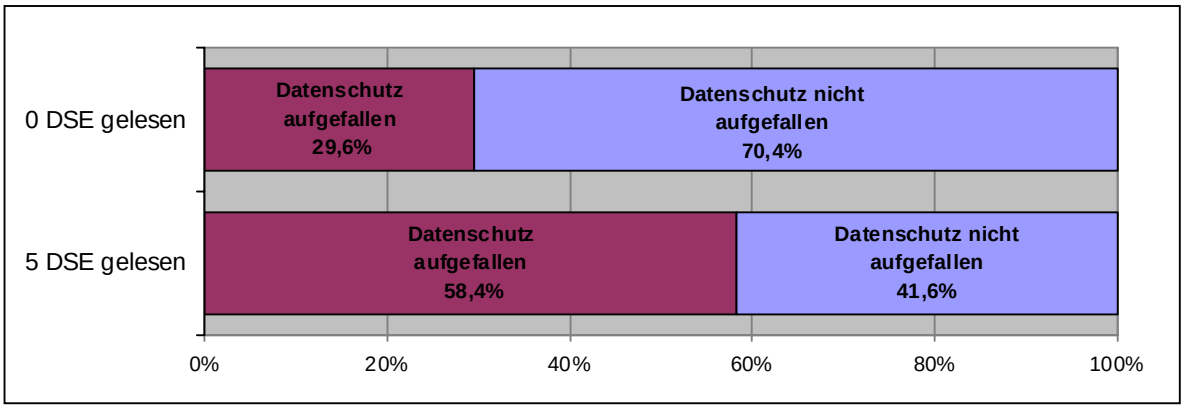
Abbildung 12: Ist den Befragten das Thema Datenschutz in Zusammenhang mit Online-Spielen aufgefallen?



Bei einer weitergehenden Betrachtung des Datenmaterials zeigt sich, dass die Teilnehmer, die von ihren „Top 5“-Spielen keine Datenschutzerklärungen gelesen haben, zum größten Teil (70,4%) auch zu dem Thema Datenschutz in Zusammenhang mit Online-Spielen nichts aufgefallen war. Dies ist nicht verwunderlich, da in den Datenschutzerklärungen der wie auch immer geartete Umgang mit den persönlichen Daten mehr oder weniger vorbildlich geregelt wird. Da den Teilnehmern nichts in Zusammenhang mit Datenschutz in Online-Spielen aufgefallen ist, kann man von einem gewissen Desinteresse oder einer Unbedarftheit zum Thema Datenschutz in Online-Spielen ausgehen. Bei den Teilnehmern, die alle fünf Datenschutzerklärungen ihrer „Top 5“-Online-Spiele gelesen haben, kehrt sich das Verhältnis um. Jedoch gibt es auch hier einen nicht unerheblichen Teil, dem Datenschutz in Zusammenhang mit Online-Spielen noch nicht aufgefallen ist. (Siehe Abbildung 13.)

[164] Pressemitteilung der Verbraucherzentrale Schleswig-Holstein vom 11.08.2008, Callcenter sind im Besitz von Kontodaten – Verbraucherzentrale Schleswig-Holstein deckt Datenmissbrauch auf, Abrufbar unter: http://www.verbraucherzentrale-sh.de/UNIQ125085673012315/link481821A.html.
Pressemitteilung des Unabhängigen Landeszentrum für Datenschutz, Datenhandel: „Die sichtbare Spitze des Eisbergs wird größer“ – neue illegale Datensätze aus Callcenter aufgetaucht, Abrufbar unter: https://www.datenschutzzentrum.de/presse/20080818-datenhandel-callcenter.htm.

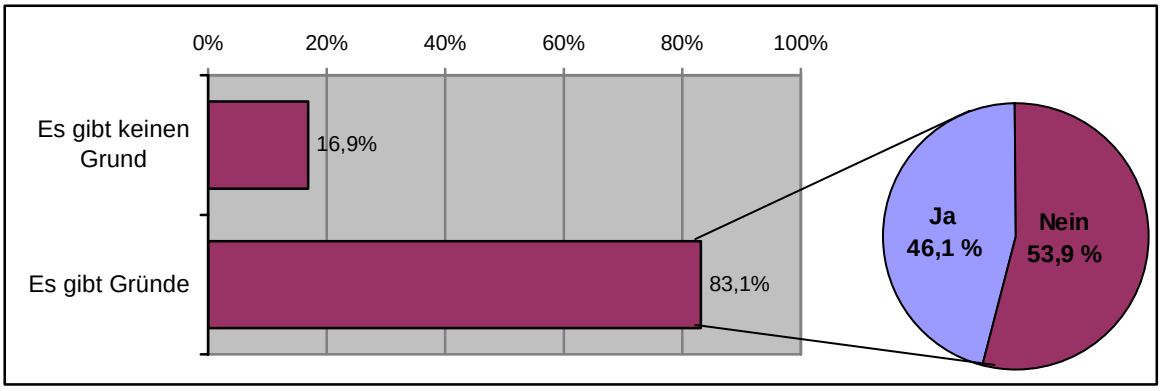
Abbildung 13: Verhältnis von gelesenen Datenschutzerklärungen zu der Wahrnehmung von Datenschutzproblematiken



In der Gruppe der Teilnehmer, für die es Datenschutzgründe gibt, ein Online-Spiel nicht zu nutzen (siehe Abbildung 10), ergab eine weiterführende Analyse, dass 46,1% schon einmal Datenschutz in Zusammenhang mit Online-Spielen aufgefallen ist; dagegen ist den verbleibenden 53,9% der Themenbereich Datenschutz in Zusammenhang mit Online-Spielen noch überhaupt nicht aufgefallen. (Siehe Abbildung 14.)

Obwohl mehr als der Hälfte der Teilnehmer noch kein Datenschutzthema in Zusammenhang mit Online-Spielen aufgefallen ist, gibt es aus ihrer Sicht doch mögliche Gründe, um Online-Spiele nicht zu nutzen. Dieses liegt möglicherweise an den Datenschutzskandale der jüngsten Zeit und dem Misstrauen der Verbraucher gegenüber der Industrie.

Abbildung 14: Datenschutzgründe, ein Online-Spiel nicht zu nutzen, in der Verbindung zu der Wahrnehmung von Datenschutzproblematiken

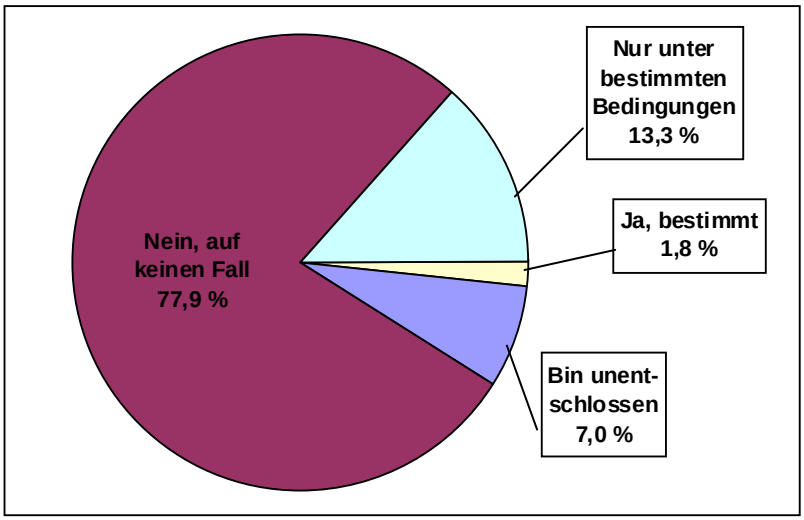


Zum Ende des Fragebogens wurden die Fragen auf das Thema Datenschutz zugespitzt und konkrete Szenarien in die Fragen eingebunden.

Eine Frage beschäftigt sich mit der Datenweitergabe, die bereits bei einer der vorangehenden Fragen als ein Grund für die Nichtnutzung von Online-Spielen identifiziert wurde. Es

wurde erhoben, ob die Befragten zustimmen würden, wenn ein Online-Spiele-Betreiber Daten über sie und ihr Spielverhalten (Spielerprofil) an Werbetreibende weitergeben möchte, sofern hierzu eine Wahl besteht. Der überwiegende Teil der Befragten (77,9%) verneinten die Frage eindeutig, nur 1,8% würden diesem Vorgehen uneingeschränkt zustimmen. 7,0% zeigten sich unentschlossen, und 13,3% würden diesem Vorgehen nur unter bestimmten Bedingungen zustimmen. (Siehe Abbildung 15.)

Abbildung 15: Zustimmung zur Weitergabe von Daten über Spieler und Spielverhalten an Werbetreibende durch den Online-Spieleanbieter

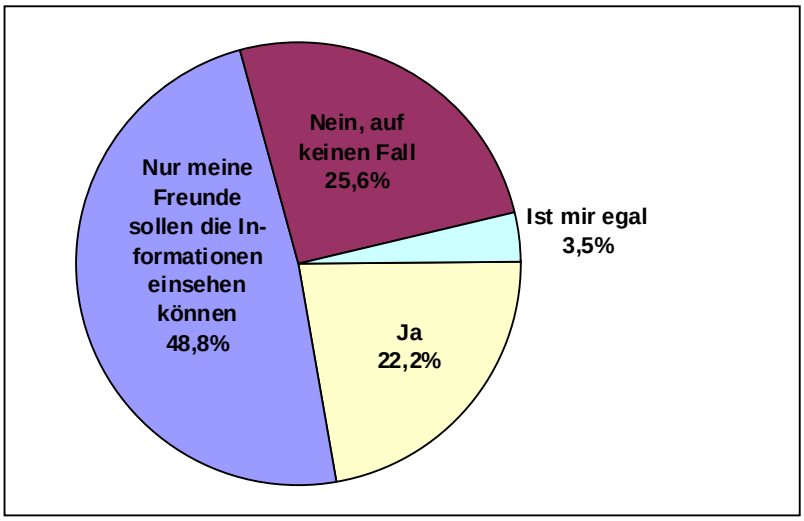


Bei der darauffolgenden Frage ist das Ergebnis etwas weniger eindeutig, zeigt aber dieselbe Tendenz: Die Befragten möchten nicht, dass ihre persönlichen Daten unkontrolliert an die Öffentlichkeit gelangen.

Die Teilnehmer der Umfrage wurden befragt, ob sie anderen Spielern erlauben würden, ihr persönliches Spielerprofil mit Informationen über gespielte Spiele, Spielzeiten und erreichte Spielergebnisse abrufen zu dürfen. 25,6% antworteten „Nein, auf keinen Fall“, weitere 48,8% könnten sich vorstellen, dass nur Freunde diese Daten einsehen können; nur 22,2% würden die Daten ohne Einschränkungen zum Abruf freigeben. 3,5% ist es egal, ob die Daten zum Abruf für jedermann bereitgestellt werden. (Siehe Abbildung 16.)

Die letzten beiden Ergebnisse lassen vermuten, dass ein Großteil der Befragten seine persönlichen Daten, die im Zusammenhang mit Online-Spielen anfallen, bei der Werbeindustrie nicht gut aufgehoben wähnt, jedoch die Daten bei den eigenen Freunden in vertrauensvollen Händen sieht.

Abbildung 16: Erlaubnis für andere Spieler, das eigene persönliche Spielerprofil abrufen zu dürfen



Kurz vor dem Ende des Fragebogens wurden den Teilnehmern der Befragung mehrere Aussagen (Statements) zur Auswahl gestellt, zwischen denen sie sich entscheiden sollten. Diese Statements sollten die persönliche Einstellung zum Thema Datenschutz in Online-Spielen widerspiegeln.

Bei der ersten Gruppe von Aussagen standen die folgenden Möglichkeiten zur Verfügung:

- „Beim Spielen möchte ich gerne anonym bleiben bzw. nur unter einem (oder mehreren) Spielernamen auftreten."
- „Ich möchte gerne, dass mich jeder beim Spielen erkennt und meinen echten Namen weiß."
- „Ich stimme keiner der beiden Aussagen zu."

Bei der zweiten Gruppe von Aussagen standen die folgenden Möglichkeiten zur Verfügung:

- „Als Spieler habe ich nichts zu verbergen."
- „Ich möchte gerne stets selber bestimmen können, welche Spieldaten von mir von wem gesehen und genutzt werden dürfen."
- „Ich stimme keiner der beiden Aussagen zu."

Dabei zeigen die Ergebnisse deutlich, dass die Teilnehmer der Befragung einen selbstbestimmten Umgang mit ihren Daten wünschen. Der Großteil hat sich für die Statements „Beim Spielen möchte ich gerne anonym bleiben bzw. nur unter einem (oder mehreren) Spielernamen auftreten." mit 79,1% (siehe Abbildung 17) und „Ich möchte gerne stets selber bestimmen können, welche Spieldaten von mir von wem gesehen und genutzt werden dürfen." mit 89,7% (siehe Abbildung 18) entschieden. Die Nennungen für die anderen Aussagen sind vernachlässigbar klein mit Ausnahme der Aussagegruppe zur Anonymität bzw. Erkennbarkeit beim Spielen, bei der das Statement „Ich stimme keiner der beiden Aussagen zu" fast

ein Fünftel aller Nennungen erhielt (siehe Abbildung 14). Dies lässt vermuten, dass einige der Befragten ihre persönliche Meinung zwischen den beiden Extremen „vollständige Anonymität“ und „vollständige Erkennbarkeit“ einordnen würden. In Verbindung mit der zweiten Aussagegruppe wird klar, dass im Vordergrund die situationsabhängige Selbstbestimmung auch über Anonymität und Erkennbarkeit steht.

Abbildung 17: Statement 1

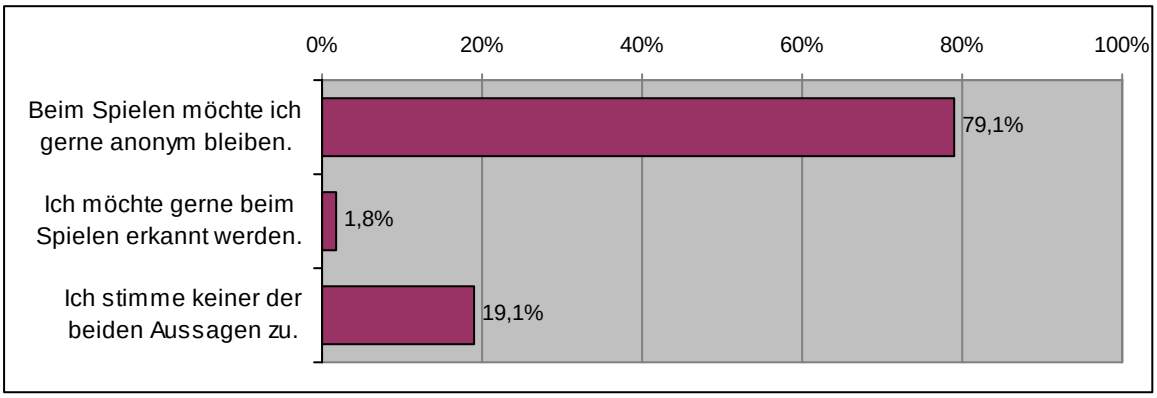
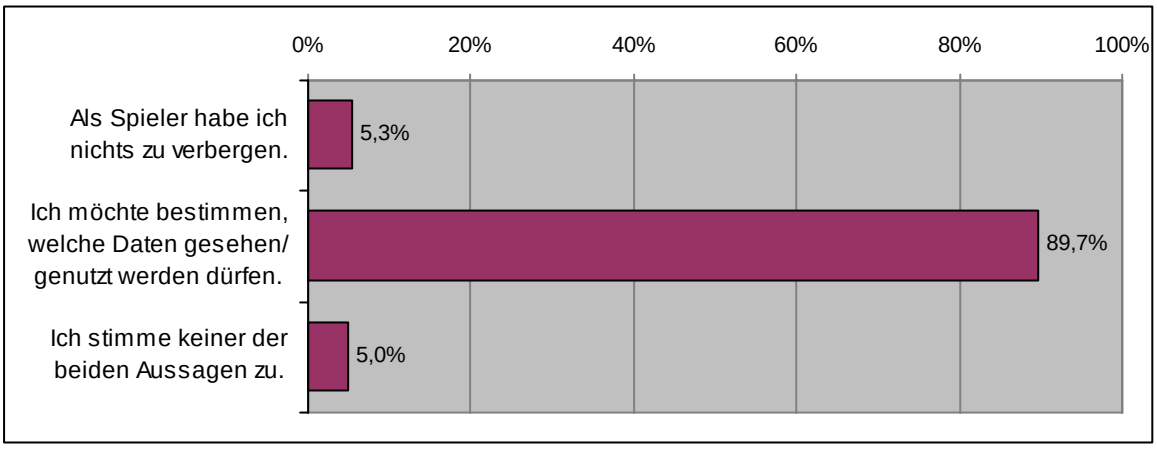


Abbildung 18: Statement 2



10.3.4 Zusammenfassung der Ergebnisse

Es lässt sich zusammenfassend feststellen, dass von den 1213 ausgefüllten Fragebögen nur ein kleiner Teil von Personen unter 18 Jahren zur Verfügung gestellt wurde. Des Weiteren zeigte sich, dass die Spieler, die an der Umfrage teilgenommen haben, Online-Spiele im gemäßigten zeitlichen Umfang nutzen und nicht zu den exzessiven Online-Spielern gehören.

Die von den Teilnehmern an der Befragung bevorzugten Online-Spiele und die in den Haushalten vorhandenen und online genutzten Geräte entsprechen den gängigen am Markt angebotenen Produkten.

Bei der Analyse des Datenmaterials ließ sich feststellen, dass dem größten Teil der Befragten der Datenschutz im Kontext mit Online-Spielen sehr wichtig ist. Die meisten Spieler legen darauf Wert, dass vertrauensvoll mit den Spielerdaten umgegangen wird, diese nicht an die Werbeindustrie weitergegeben werden und nicht von jedem im Internet abgerufen werden können. Es scheint, als wüssten die Teilnehmer an der Befragung um die Brisanz der im Zusammenhang mit Online-Spielen anfallenden Daten, wie z. B. Adress- und Kontodaten sowie vielfältige Spielerprofile, die unter anderem Informationen über gespielte Spiele, Spielzeiten und erreichte Spielergebnisse enthalten können.

Erfreulich ist, dass es für mehr als drei Viertel der Befragten Datenschutzgründe gibt, ein Online-Spiel nicht zu nutzen. Doch diese Erkenntnis führt nicht dazu, dass die Befragten sich im selben Maße den Datenschutzerklärungen der Spiele widmen und prüfen, ob die Unternehmen vertrauenswürdig mit den Daten umgehen. Dies könnte unter anderem an der Gestaltung von vielen Datenschutzerklärungen liegen. Diese zeichnen sich nicht selten dadurch aus, dass sie sehr lang, unübersichtlich und dem typischen „Kleingedruckten“ entsprechen und dem Leser so nicht wirklich Lust auf das Lesen der Datenschutzerklärung machen.

Doch auch wenn die Befragten die Spieldaten für sensible Daten halten, so sollen diese nicht für alle Gruppen tabu sein. Vielmehr zeigen die von den Befragten zum Schluss der Befragung ausgewählten Statements, dass sie einen vertrauenswürdigen und selbstbestimmten Umgang mit den Spieldaten wünschen. Die Befragten möchten zum überwiegenden Teil anonym spielen und nur unter Spielernamen auftreten, zum anderen möchten sie selbst bestimmen können, welche Spieldaten von wem gesehen und genutzt werden können.

11 Datenschutz in Online-Spielen – eine sozioökonomische Betrachtung

Computerspiele in einer verblüffenden Realitätsnähe und die multimediale Interaktion mit anderen Spielern rund um den Erdball gehören heutzutage zur Freizeitgestaltung eines Heranwachsenden. Diese Selbstverständlichkeit, mit der Computerspiele einen Platz in unserer Gesellschaft eingenommen haben, soll als Anlass dazu dienen, die sozioökonomischen Auswirkungen Online-Spielen und Datenschutz zu betrachten.

11.1 Die Welt der Online-Spieler

Die Welt, in die Computerspieler heutzutage eintauchen, bedeutet für viele junge Menschen einen besonderen Reiz. Für einen Außenstehenden mag ein Computerspiel als eine sinnentleerte Interaktion mit einer Maschine erscheinen. Doch mittlerweile zeichnen sich heutige Computerspiele durch eine Vielzahl von Interaktionsmöglichkeiten mit anderen realen Mitspielern und medialer Realitätsnähe aus. Die Spieler spielen nicht nur, sie schlüpfen in Rollen, die ganz außergewöhnlich sein können, und sie agieren und verhalten sich entsprechend den erwarteten oder auch erst noch zu erarbeitenden Rollenmustern. Dabei kann jeder die Rolle auswählen, in die er schlüpfen oder die er gestalten möchte. Die breite Palette an Computerspielen bietet fast jedem die Möglichkeit, eine Rolle nach den eigenen Bedürfnissen zu finden. Wenn es ein Kennzeichen der modernen Gesellschaft ist, dass Menschen besonders viele und nicht unbedingt leicht zu vereinbarende Rollen spielen und für sich plausibel machen, so passt diese qualitative und quantitative Ausweitung des Rollensets über Computerspiele in diese Entwicklung menschlicher Gesellschaften plausibel hinein. Die Menschen spielen immer komplexere Spiele und treten dabei mehr in Interaktion mit anderen Spielern. Das Anrüchige, das den Computerspielen anhaftet, mag daraus resultieren, dass das Spielen als etwas Anderes zu in unserer Gesellschaft als wichtig empfundenen und hochgeschätzten Arbeit gilt. Und wenn das Spiel als so anstrengend wahrgenommen wird, dass es offenbar nicht als Erholung zum Nutzen der Fortführung der Arbeit gelten darf, dann verbleiben zwei kulturell stark verwurzelte Strategien des Umgangs damit: Entweder wird das Spielen gebannt und Spieler gelten als pathologisch, oder es wird eben doch ein Nutzen zweiter Ordnung vermutet, nämlich dass ganz neue Fertigkeiten im Spielen trainiert werden, die in modernen Arbeitszusammenhängen eine wichtige Funktion haben. Letzteres scheint bei uns heute der Fall zu sein. Denn die Computerspiele erzeugen Spielerprofile, die detailliert Auskunft über Eigenschaften eines Spielers geben können. Und der Umgang insbesondere mit solchen Profilen ist ein datenschutzrechtlich bedeutsames Problem.

Computerspiele zeichneten sich vor einigen Jahren noch hauptsächlich dadurch aus, dass sich hinter den Gegnern im Spielgeschehen bzw. weiteren Teampartnern nur der Computer mit der Abarbeitung zwar unterschiedlicher, aber doch letztlich recht einfacher Algorithmen verbarg. Mit dem Internet und der weltweiten Vernetzung wurden dann die meisten Computerspiele mit Online-Funktionalität ausgestattet, so dass auch unerwartete, überraschende,

interessante Interaktionen in Computerspielen entstanden. Diese Möglichkeit der Vernetzung von Spielern war insofern ein dramaturgischer Meilenstein in der Welt der Computerspiele. Es kann sich bei einem Gegner im Spiel durchaus um einen Freund handeln, der eine Straße entfernt vor seinem Computer sitzt, oder um eine nicht näher bekannte Person auf der anderen Seite der Weltkugel. Durch die neuen Interaktionsmöglichkeiten und die weiterentwickelten Multimediaeffekte steigt die Realitätsnähe, man kann sich mit realen Mitspielern im Spiel messen und gemeinsam im Spiel taktieren, besser und realitätsnäher als mit jedem Computergegner. Insofern vereinsamen Online-Spieler in der Interaktion mit dem Computer sozial nicht zwangsläufig. In den Online-Spielen mit Mehrspielermodus bilden sich unter den Spielern Clans, die zusammen in dem Online-Spiel als Team fungieren. Untersuchungen belegen, dass ein Großteil der Spieler sich untereinander in der „Offline-Welt“ trifft[165] und dabei auf althergebrachte Art soziale Kontakte pflegt.

11.2 Der Wirtschaftsfaktor Online-Spiele

Die Erfolgsmeldungen für das Online-Spiele-Geschäft reißen nicht ab. Die großen Neuerscheinungen auf dem Online-Spiele-Markt übertreffen sich regelmäßig mit Verkaufszahlen und Umsatzerlösen. Spielkonsolen und Computerspiele sind keine namenlose Massenware, sondern Neuerscheinungen werden sehnsüchtig von den Fans erwartet.[166] In Deutschland werden jährlich etwa 2,7 Mrd. Euro im Bereich der elektronischen Spieleindustrie umgesetzt, zusätzlich machen zweistellige Jahreswachtumsraten diesen Zweig zu dem Bedeutendsten der Unterhaltungsbranche.[167] Es gibt schätzungsweise 10.000 Arbeitsplätze im Bereich der Spieleproduktion in Deutschland.[168]

Die Online-Spiele haben es, im Unterschied zu den herkömmlichen Computerspielen ohne Online-Funktionalität, geschafft, zusätzlich zum Verkaufspreis alternative Monetarisierungsmodelle und eine Reihe zusätzlicher kostenpflichtiger Wertschöpfungsprozesse zu etablieren. So lassen sich viele der großen Online-Spiele nur im Rahmen eines monatlichen Abonnements spielen und sorgen so für regelmäßige Einnahmen beim Publisher/Betreiber. Neben diesen primären Umsätzen durch Verkäufe der Spiele und Abonnement-Systeme sind weitere Profitbereiche im Spiel bzw. Spielumfeld erschlossen worden. Dazu gehören unter anderem In-Game-Advertising, Merchandising oder Umsätze durch den Verkauf von virtuellen Gegenständen im Spiel.

Die Nutzer von digitalen Spielen bilden eine interessante Zielgruppe für die Werbe-

[165] Sozioland, Tabellenband Sozioland Games 2008, S. 78f.

[166] Spiele Picken, Logistik Heute 6/2009, S. 20-21, S. 20.

[167] BITKOM / Deloitte, Spielend unterhalten – Wachstumsmarkt Electronic Games – Perspektive Deutschland, S. 8.

[168] Bundesverband Interaktive Unterhaltungssoftware e.V., http://www.biu-online.de/fakten/gamesbranche/.

industrie.[169] Die Computerspielbranche hat diesen Umstand erkannt und die Werbebotschaften mit verschiedenen Konzepten in die Spiele integriert. Diese Vermarktungsform wird mit dem Begriff In-Game-Advertising bezeichnet. In die Spiele werden beispielweise Werbebotschaften eingebunden, die statisch eingeblendet oder dynamisch, aufgrund von Spielerprofilen, kontextsensitiv ins Spiel eingeblendet werden. Die Werbung kann somit auf den Spieler zugeschnitten eingebunden werden. Einige Spielideen und -konzepte sind so konzipiert, dass die Spieler nicht für die Nutzung Geld zahlen. Das Geschäftsmodell basiert hier auf den Einnahmen über Werbung.

Des Weiteren werden Spielwährungen in das Spielkonzept und Spielgeschehen integriert, wobei das „virtuelle Geld“ im Spielgeschehen erarbeitet und/oder im Tausch gegen reale Währungen erworben werden können. Die Währungen dienen unter anderem dazu, im Spiel die Spielfigur mit virtuellen Gegenständen auszustatten. Mehr als ein Drittel der Besucher von virtuellen Welten haben bereits reale Käufe vollführt, um die Waren in virtuellen Welten zu verwenden.[170] Die Umsätze aus diesem Bereich beliefen sich im Jahre 2007 auf eine Summe von fast 2 Mrd. US-Dollar, wobei es sich um reale Geldbewegungen handelte und nicht um „Spielgeld“.[171]

Um den Bereich Computer- und Online-Spiele ranken sich auch eine Reihe von Zeitschriften und Fernsehformate, die die Thematik eines Spiels als Trägerthema für ihre Werbung entdeckt haben. Einzelne Zeitschriften zum Thema Computerspiele haben Auflagen von weit mehr als 250.000 und erreichen darüber ein Vielfaches an Lesern. Zumeist ergänzen die Zeitschriften ihren Auftritt mit einem Online-Portal und können darüber wiederum weitere Einnahmen durch darauf geschaltete Online-Werbung realisieren.

Wie bei vielen erfolgreichen Produkten mit Fankultur gibt es auch im Bereich der Computer- und Online-Spiele ein großes Merchandising-Programm. Dem Produktumfang sind dabei keine Grenzen gesetzt. Das Merchandising ist bei einigen Kinofilmen oder Musikkünstlern so erfolgreich, dass die Merchandising-Einnahmen die Einspielergebnisse des eigentlichen Produkts übertreffen. Somit dürfte das Merchandising auch im Bereich der Online-Spiele für zusätzliche Geldflüsse sorgen.

Insgesamt stellt also der Markt für Online-Spiele mit seinen angrenzenden Vermarktungsbereichen einen nicht unerheblichen Wirtschaftsfaktor dar. Die Spielergemeinde ist bereit, für das interessante Hobby entsprechend Geld auszugeben. Damit sind die Spieler eine kaufkräftige Zielgruppe für die Werbeindustrie bzw. die dahinterstehenden werbenden Unternehmen.

---

[169] Schulze / Jöckel / Will, Grundlagen der Werbewirkungsforschung für Ingame-Advertising, in: Menschen Märkte Medien Management – Berichte aus Forschung und Lehre 01/2007, TU Ilmenau, S. 5.

[170] ENISA; Survey Results – Security And Privacy In Massively-Multiplayer Online Games And Social And Corporate Virtual Worlds, 2008, S. 14.

[171] ENISA, Virtual Worlds, Real Money, 2008, S. 9.

11.3 Datenschutz als Prozess im Unternehmen

Die sozioökonomischen Auswirkungen des Datenschutzes auf den Online-Spielebereich ist ein meist unterschätzter und deshalb bisher wenig diskutierter Bereich.

Datenschutz bzw. das allgemeine Persönlichkeitsrecht gehört in Deutschland zu den am höchsten im Grundgesetz verankerten Grundrechten eines Bürgers. Jeder soll einschätzen können, wer was wann über ihn weiß. Dies bedeutet, dass ein Bürger, ebenso wie ein Kunde und Patient, wissen können soll, welche Daten über ihn staatliche Verwaltungen, Unternehmen und Institute, Internet-Provider und Energieversorgungsunternehmen sowie Vereine oder auch die Arbeitgeber speichern und verarbeiten.

Der Bürger bzw. Kunde, der Online-Spiele in seiner Freizeit spielt, verlässt sich in der Regel pauschal darauf, dass seine Daten entsprechend den geltenden Datenschutzgesetzen geschützt sind bzw. geschützt und entsprechend vertraulich behandelt werden: Dazu gehören die persönlichen Daten, die erhoben werden, um zum Spiel zugelassen zu sein, das Spielerprofil und die während des Spiels aufgezeichneten Aktivitäten sowie die Internet-Verbindungsdaten, um nur die wichtigsten zu nennen. Auch Unternehmen vertrauen darauf, dass bei anderen Beteiligten Rechtssicherheit darüber herrscht, welche Vorgaben das Unternehmen bzw. die Produkte erfüllen müssen, damit sie u. a. den datenschutzrechtlichen und datensicherheitstechnischen Vorgaben genügen. Dies ermöglicht es den Unternehmen, dafür entsprechende Aufwände zu kalkulieren.

Datenschutz ist eine Größe, die von Unternehmen in ihren Kosten- und Unternehmenssteuerungssystemen abgebildet werden kann. Wurde Datenschutz früher gerne als reiner Kostenfaktor gesehen, der keinen bzw. einen nur geringen Return-of-Investment versprach, so dürfte es sich heute kein Unternehmen mehr leisten können, den Datenschutz im Unternehmen zu vernachlässigen.[172] Eine US-Studie hat festgestellt, dass sich die Kosten für einen verlorenen Datensatz im Durchschnitt auf 202 US-Dollar belaufen; dabei sind juristische Konsequenzen noch nicht berücksichtigt. Der Verlust oder Diebstahl eines Laptops mit Unternehmensdaten führt zumeist dazu, dass Tausende von Datensätzen abhanden kommen. Die dabei entstehenden Schadenssummen können bei 202 US-Dollar pro Datensatz somit schwindelerregende Höhen erreichen.[173] Der Verlust von Laptops ist keine Seltenheit; an europäischen Flughäfen wird Woche für Woche der Verlust von mehreren Tausend Laptops registriert.[174] Sollte die breite Öffentlichkeit von solchen Datenpannen aufgeschreckt werden, so dürften die Unternehmen besonders unter einem möglichen Imageverlust leiden.

---

[172] Borchers, Datenschutzmanagement als Wettbewerbsfaktor in IT-Sicherheit & Datenschutz 11/2006, S. 721-724, S. 721f.

[173] Ponemon Institute, Fourth Annual US Cost of Data Breach Study, Januar 2009.

[174] An den größten 8 europäischen Flughäfen ist der Verlust von durchschnittlich 3.300 Laptops pro Woche zu beklagen. Ponemon Institute, Airport Insecurity: The Case of Lost & Missing Laptops, Juli 2008.

Im Rahmen von Online-Spielen werden viele personbezogene Daten erhoben und verarbeitet. Die derzeit erfolgreichsten Online-Spiele zeichnen sich dadurch aus, dass sie von Spielern vielfältige Fähigkeiten beim Spielen einfordern. Die Spiele verlangen unter anderem Taktik, Logik und Strategie, Schnelligkeit und Problemlösungsfähigkeiten. Die während des Spielens anfallenden Daten spiegeln die Ausprägung derartiger Anforderungen bzw. Fähigkeiten wider. Diese Daten können zu Spielerprofilen zusammengeführt werden und erzeugen spätestens dann sensible Datenbestände, wenn sie mit den dahinterstehenden realen Personen verkettet werden können oder verkettbar sind.[175] Mit jedem neuen Datum reift ein solches Spielerprofil, das man insgesamt als ein kognitiv-biometrisches Merkmal des Spielers charakterisieren kann. Aus solchen Profilen ergibt sich, wie jemand in bestimmten Situationen agiert, wie schnell er sich in neue Aufgabenstellungen eindenken und diese bewältigen kann, wie jemand in bestimmten Situationen taktiert, eher angreifend oder eher verteidigend, und ob jemand ein Teamplayer oder ein Einzelkämpfer ist, ob jemand Rücksicht übt oder allein auf die Maximierung der eigenen Effizienz achtet.

Die Spielsituationen in Online-Spielen entsprechen sicherlich nicht der Realität. Aber das Ausgesetztsein und Einüben der dabei stattfindenden Interaktionen zwischen den Spielern kann sich als Erfahrung auch im Leben außerhalb der Rechner auswirken. Interessenten für solche Daten zu finden, sollte nicht schwer sein. Heutzutage versuchen Unternehmen beispielsweise, in langwierigen Assessment-Centern herauszufinden, welcher Bewerber für die vakante Stelle eines Managers oder Gruppenleiters geeignet ist. In Zukunft wird vielleicht das Spielerprofil eine Antwort darauf liefern: Wer in einem Team eines MMOG die Führungsrolle übernimmt und die Mission zielgerichtet ohne große Umwege zum Erfolgt führt, ist möglicherweise ein besserer Abteilungsleiter als eine Person, die es in der gleichen Spielsituation als Einzelkämpfer versucht.

Im Rahmen von Online-Spielen fallen große Mengen von personenbezogenen Daten an, so dass es den Herstellern und Betreibern von Online-Spielen obliegt, diese Daten entsprechend den gesetzlichen Regelungen zu schützen. Die Kosten verursachenden Maßnahmen zum Datenschutz und zur Datensicherheit können dadurch niedrig gehalten werden, indem Datenschutz in die Prozesse des Qualitätsmanagements im Rahmen des Compliance-Managements integriert werden.[176] Dies betrifft alle Bereiche eines Unternehmens und alle Produktlebenszyklen, von der Entwicklung eines Online-Spiels bis hin zum Kundensupport. Das wesentliche gesetzliche Regularium des Datenschutzes ist die Zweckbindung einer Datenverarbeitung. In Bezug auf das Ermöglichen von Spielen dürfen Daten aus den Spielen zu nichts anderem als genau dazu, nämlich dem Ermöglichen des Spielens, genutzt werden. Alles andere bedürfte einer wirksamen Einwilligung durch den Spieler. Derartige Einwilligungserklärungen findet man in Online-Spielen bislang aber so gut wie nie.

---

[175] Eine umfassende Darstellung zur Verkettbarkeit von Daten enthält der Report „Verkettung digitaler Identitäten“ des Unabhängigen Landeszentrums für Datenschutz in Zusammenarbeit mit der Technischen Universität Dresden im Auftrag des Bundesministeriums für Bildung und Forschung; 2007. S. 19ff.

[176] Bizer, Datenschutz in die Prozesse, in: DuD 10/2006, S. 598.

In den Unternehmen, die Spiele herstellen oder Spielplattformen/Spielsysteme hosten, sollten Datenschutzmanagementprozesse eingezogen werden, die – ebenso wie die anderen Prozesse eines Unternehmens – über Key Performance Indikatoren (KPI) beobachtet und gesteuert werden. Diese KPI sollten sich an den Schutzzielen für Datensicherheit (insbesondere Vertraulichkeit, Integrität, Verfügbarkeit) und Datenschutz (insbesondere Transparenz, Kontingenz, Nichtverkettbarkeit) ausrichten.[177] Außerdem lassen sich empirische Daten in Bezug auf Datenschutzthematisierungen nutzen: Wie viel Datenschutzanfragen bzw. Vorfälle wurden in einem bestimmten Zeitraum gemeldet, und wie schnell und nachhaltig wurden diese Vorfälle bearbeitet? In welchem Maße werden die Dokumentations- und Protokollierungsanforderungen gemäß Anhang zu § 9 BDSG erfüllt? Damit steht, neben dem finanziellen Aspekt, der Datenschutz als wesentliche Komponente des Compliance-Managements im Fokus der Unternehmensführung.

Ein optimal in die Unternehmensprozesse integriertes Datenschutzmanagement macht Prozesse als Verfahren transparent und ist dadurch ein ganz wesentlicher Erfolgsfaktor in Bezug auf Führbarkeit und Kontrolle eines Unternehmens. Die Qualität des Umgangs mit personenbezogenen Daten im Unternehmen ist ein Indikator für die kontrollierte Qualität der Datenverarbeitung überhaupt. Diese Qualität erstreckt sich dabei insbesondere bis zum Datenschutz auch für die Mitarbeiter des Unternehmens.

Die Umfrage im vorangegangen Kapitel hat gezeigt, dass die Befragten bei Online-Spielen großen Wert auf einen vertrauensvollen Umgang mit persönlichen Daten legen. Unternehmen, die den Datenschutz vorbildlich umgesetzt haben, sollten eine Zertifizierung mit einer entsprechenden Außenwirkung anstreben. Dafür kommen das Datenschutz-Gütesiegel auf Grundlage des schleswig-holsteinischen Landesdatenschutzgesetzes und das European Privacy Seal (EuroPriSe) als Qualitätssicherungs- und Marketinginstrument in Frage. Beide Verfahren prüfen in einem zweistufigen Verfahren, unter Einbindung externer Sachverständiger, die Einhaltung der gesetzlichen Normen im Hinblick auf Datenschutz und Datensicherheit bei IT-Produkten. Nach erfolgreicher Prüfung wird den Produkten das Datenschutz-Gütesiegel bzw. EuroPriSe-Siegel verliehen, das den Unternehmen die Möglichkeit gibt, damit gegenüber den Kunden zu werben und in die Marketingaktivitäten zu integrieren.

[177] Rost / Pfitzmann, Datenschutz-Schutzziele – revisited, in: DuD 06/2009, S. 353-358.

12 Datenschutz als Geschäftsmodell

12.1 Einleitung

Die Entwicklung von Geschäftsmodellen im Bereich Datenschutz für Online-Spiele ergibt nur einen nachhaltigen Effekt, wenn die Wertschöpfung auf Kunden- und der Ertrag auf Anbieterseite positiv ausfallen. In diesem Business-to-Business-Sektor stehen im Bereich der Online-Spiele auf der Kundenseite Hersteller, Publisher oder Betreiber; auf der Anbieterseite stehen Dienstleister, die entsprechende Produkte oder Dienstleistungen anbieten (Betreiber). Für die Anbieter von Leistungen ist die Ertragsseite der ausschlaggebende Faktor. Sie werden nur Dienstleistungen anbieten, wenn sich zumindest mittel- bis langfristige Überschüsse realisieren lassen. Auf der Nachfragerseite ist der Fall etwas anders gelagert; hier ist das Entscheidungskalkül nicht nur die positive Wertschöpfung durch den Einsatz des Datenschutz-Know-hows, sondern auch die Erfüllung von gesetzlichen Regelungen und Vorgaben. Der Verstoß gegen gesetzliche Regelungen kann Bußgelder oder Imageschäden nach sich ziehen.

Die Befragung im Rahmen dieser Studie hat gezeigt, dass die Spieler einen vertrauenswürdig Umgang mit personenbezogenen Daten von Unternehmen für sehr wichtig erachten. Gleichzeitig stellt eine Untersuchung des Instituts für Demoskopie Allensbach fest, dass die meisten Deutschen (82%) den Unternehmen beim Umgang mit persönlichen Daten misstrauen.[178] Die Unternehmen haben mehr denn je die Aufgabe gegenüber ihren Endkunden, Vertrauen aufzubauen, denn die Grundlage für wirtschaftliches Handeln zwischen Käufer und Verkäufer ist Vertrauen. Die bestehenden Geschäftsmodelle und Konzepte im Bereich Datenschutz gewinnen damit mehr Aktualität und Berechtigung denn je. Die Wirtschaft hat augenscheinlich einen Nachholbedarf im Bereich Vertrauensbildung zu seinen Kunden.

12.2 Geschäftsmodelle

Im Folgenden werden Geschäftsmodelle vorgestellt, die aus Sicht des Datenschutzes Erfolg versprechend sind und das Datenschutzniveau im Bereich der Online-Spiele für die Verbraucher erhöht. Der Datenschutz wird auf diese Weise zu einem Wettbewerbsfaktor für Unternehmen.[179]

---

[178] Institut für Demoskopie Allensbach, Zu wenig Datenschutz? Die meisten sind mit persönlichen Daten vorsichtig geworden. Allensbacher Bericht Nr. 6/2009.

[179] Grundlegend Büllesbach, Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsvorteil, RDV 1997, 239f.

12.2.1 Datenschutz-Zertifizierung

Die Verbraucher fordern von Unternehmen einen vertrauensvollen Umgang mit personenbezogenen Daten der Kunden. Es gibt deshalb die Möglichkeit, den Umgang mit personenbezogenen Daten in den Unternehmen von einer unabhängigen Stelle prüfen zu lassen. Das positiv verlaufene Prüfungsverfahren kann das Unternehmen nutzen, um gegenüber den eigenen Kunden Vertrauen aufzubauen.

Es gibt bereits bestehende Zertifizierungskonzepte für Produkte im Bereich Datenschutz, die sich am Markt etabliert haben. Hierzu zählen das schleswig-holsteinische Datenschutz-Gütesiegel[180] und das europäische Datenschutz-Gütesiegel EuroPriSe (European Privacy Seal)[181]. Beide Gütesiegel setzen auf einem zweistufigen qualitätsgesicherten Prüfungsverfahren auf. In einem ersten Schritt werden die Produkte von externen anerkannten Sachverständigen überprüft und die Ergebnisse in einem Gutachten niedergelegt. Dieses Gutachten nimmt die unabhängige Zertifizierungsstelle als Grundlage für die weitere Prüfung. Bei einem positiven Ausgang der Prüfung wird im Anschluss das Datenschutzsiegel verliehen.

Das schleswig-holsteinische Gütesiegelverfahren prüft die Produkte auf Einhaltung der gesetzlichen Datenschutzregelungen in Schleswig-Holstein. Es ist in dem Landesdatenschutzgesetz Schleswig-Holstein verankert.[182] Dieses Konzept ist Vorreiter in Deutschland, und es wurde inzwischen von vielen Herstellern von IT-Produkten aus dem gesamten Bundesgebiet und der Welt genutzt, um die Datenschutzkonformität ihrer Produkte überprüfen zu lassen und den Vorteil gegenüber anderen Mitbewerbern herauszustellen. Dieses Konzept hat das europäische Datenschutz-Gütesiegel EuroPrise (European Privacy Seal) aufgegriffen und mit Förderung der Europäischen Kommission auf die Anforderungen eines europaweiten Einsatzes angepasst. Die Produkte werden dabei in einer mit dem schleswig-holsteinischen Verfahren vergleichbaren Prüfung auf die Einhaltung der europäischen Regelungen, insbesondere der Datenschutz-Richtlinien, geprüft und bei positivem Ergebnis zertifiziert.

Beide vorgestellten Verfahren bieten sich auch für den Bereich der Online-Spiele an. Der Hersteller kann seine Online-Spiele bzw. Online-Spielsystem auf Datenschutzkonformität überprüfen lassen. Zwar ist Voraussetzung für die Zertifizierung in Schleswig-Holstein, dass es zur Nutzung in einer öffentliche Stelle geeignet ist (§ 1 Abs. 2 Datenschutzauditverordnung Schleswig-Holstein). Für die meisten Online-Spiele und Systeme dürfte dieses Erfordernis jedoch erfüllt sein, wenn man bedenkt, dass diese Produkte in staatlichen Jugendheimen, Schulen und Jugendbegegnungsstätten Verwendung finden können.

---

[180] Bäumler, Marktwirtschaftlicher Datenschutz, in: DuD 06/2002, S. 325-329, S. 328f.
Schläger, Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein, in: DuD 08/2004, S. 459-461.
Weitere Informationen unter http://www.datenschutzzentrum.de/guetesiegel/.

[181] Bock, EuroPriSe – Das Datenschutz-Gütesiegel aus Schleswig-Holstein wird europäisch, in: DuD 06/2007, S. 410.
Meissner, Zertifizierungskriterien für das Datenschutzgütesiegel EuroPriSe, in: DuD 08/2008, S. 525-531.
Weitere Informationen unter http://www.european-privacy-seal.eu/.

[182] § 4 (2) LDSG Schleswig-Holstein und entsprechende Verordnung.

Bei positivem Ausgang des Verfahrens kann der Antragsteller das verliehene Siegel dazu nutzen, um gegenüber seinen Kunden damit zu werben und Vertrauen aufzubauen. Er hebt sich damit gegenüber seinen Mitbewerbern ab und macht das Thema Datenschutz in seiner Branche zu einem Thema zwischen Kunden und Unternehmen, so dass sich auch die Mitbewerber zu Datenschutz und dem Umgang mit personenbezogenen Daten positionieren müssen.

In dem zweistufigen Zertifizierungsverfahren kommen neben der Zertifizierungsstelle auch externe, von der Zertifizierungsstelle anerkannte Sachverständige zum Einsatz. Während die Zertifizierungsstelle derzeit von einer unabhängigen behördlichen Einrichtung betrieben wird (dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein), ergibt sich im Bereich der für die Zertifizierung notwendigen Sachverständigen eine Nachfrage nach kompetenten Fachleuten. Dies ist ein Geschäftsfeld für Selbstständige und Unternehmen, die im Bereich Datenschutz-Consulting von Unternehmen tätig sind.

12.2.2 Beratungsleistungen

Aufgrund der Vielzahl von Unternehmen, die sich auf dem Online-Spiele-Markt tummeln und ständig neue Spielkonzepte entwickeln, wird der Bedarf an Datenschutz-Know-how beachtlich sein. Bisher wurde die Computerspielbranche von Datenschutzskandalen verschont, doch auf dem umkämpften Markt dürfte es sich kein Unternehmen leisten können, mit Negativschlagzeilen in die Öffentlichkeit zu geraten.

Die im Rahmen dieser Studie entwickelten Datenschutzmodule sind eine erste Orientierung für Standardfälle. Die Realität hält jedoch Sonderfälle bereit, die zu weiterem Beratungsbedarf führen. Für die Beratung kommt zum einen eine regelmäßige und ganzheitliche Betreuung des Unternehmens in Form eines externen Datenschutzbeauftragten in Frage. Zum anderen ist auch eine projektabhängige, zeitlich begrenzte Unterstützung beispielweise während der Entwicklung neuer Technologien oder Funktionen denkbar. Generell ist es Aufgabe bei der Beratung, ein Datenschutzbewusstsein beim Auftraggeber zu entwickeln, Problembereiche zu identifizieren, datenschutzkonforme Lösungen zu finden und, kurz gesagt, sicherzustellen, dass nicht gegen die Regeln des Datenschutzes verstoßen wird[183].

Aus dem hohen Beratungsbedarf ergibt sich implizit ein entsprechender Schulungs- und Fortbildungsbedarf.

12.2.3 Produkte auf Komponentenbasis

Die Hersteller, Publisher und Betreiber von Online-Spielen werden ein Interesse daran haben, für spezielle Anwendungsbereiche fertige Komponenten zuzukaufen, die die Anforde-

[183] Ausführlich Weichert, Datenschutzberatung – Hilfe zur Selbsthilfe, in: Bäumler, Der neue Datenschutz, S. 213 ff.

rungen des Datenschutzes und der Datensicherheit vorbildlich umsetzen. Die Integration solcher Komponenten erspart es dem Entwickler, für jede Anforderung selbst aufwendige Lösungen zu entwickeln.

So ergibt sich ein weiteres gewinnversprechendes Betätigungsfeld für Unternehmen. Es gilt dabei Komponenten für den Online-Spielebereich zu entwickeln, die sich unter anderem durch eine datenschutzkonforme Datenverarbeitung auszeichnen. Die Hersteller und Betreiber von Online-Spielen müssen sich dann nicht mit zeit- und kostenintensiver Entwicklung eigener Lösungen beschäftigen. Sie können diese Aufgaben outsourcen, auf angebotene Komponenten zurückgreifen und diese in ihre Produkte integrieren. Den Anbietern der Komponenten obliegt dabei eine Informations- und Beratungspflicht, um bei der Anpassung der Komponenten keine neuen potentiellen Fehlerquellen bei der Verarbeitung von personenbezogenen Daten zu implementieren.

Es ist dabei ein höheres Datenschutzniveau im Bereich der Online-Spiele zu erwarten. Die Anbieter der Komponenten können sich auf ihre Kernkompetenz konzentrieren und solche Komponenten entwickeln, die sich einfach in bestehende Produkte bzw. Produktideen einbinden lassen sowie die rechtlichen Anforderungen erfüllen. Dazu gehören neben dem Datenschutz auch andere Fachbereiche wie beispielsweise der Jugendschutz. Ein solches Konzept führt zur Bildung von Fachwissen in der Wechselwirkung von Datenschutz und der der betreffenden Komponente. Auf der Seite der Online-Spiele werden ausgereifte und rechtlich vorbildliche Lösungen zum Vorteil der Spieler angeboten.

Beispiele hierfür sind bereits am Markt zu beobachten. Dazu gehören unter anderem Bezahlsysteme, die auf Prepaid-Karten beruhen.

Im Bereich der Online-Spiele bieten zumeist Publisher und Betreiber von Online-Spielen ihre Leistungen gegen Bezahlung an. Obwohl die Leistung (z. B. der Download eines Spiels oder Erwerb von Spielwährung) meistens keine Identifizierung des Spielers erfordert, wird diese durchgeführt, da die meisten konventionellen Zahlungssysteme (Kreditkarte oder Überweisung) eine Identifizierung des Käufers notwendig machen. Der eigene Aufbau eines anonymen Zahlungssystems ist für die einzelnen Hersteller und Betreiber von Online-Spielen zu aufwendig und kostenintensiv. Eine Möglichkeit bietet ein Konzept auf Basis von Prepaid-Karten[184], die im Barverkauf veräußert werden. Der Barverkauf sichert dem Käufer die Anonymität beim Verkaufsvorgang. Dieses Konzept erfordert jedoch ein bundesweites Netz von Verkaufsstellen; diese Infrastruktur ist entsprechend aufwendig zu realisieren. Eine solche Lösung ist prädestiniert, um sie als Hersteller oder Betreiber von einem dritten Anbieter einzukaufen und in die eigenen Produkte zu integrieren. Um eine vollständige Anonymität des Spielers zu gewährleisten, ist die Zahlungsproblematik allerdings nur ein Baustein und erfordert weiterreichende Maßnahmen.

Eine weitere Dienstleistung besteht in der Bereitstellung von Anonymitätsdiensten bzw. Ano-

[184] Die Prepaid-Karte enthält einen Code, der ein definiertes Guthaben freischaltet und entsprechend abbucht.

nymisierungs-Proxies. Diese verhindern, dass die Betreiber des Spiels die IP-Adresse des Nutzers und ggf. weitere identifizierende Informationen wie den Referer der Anfrage erhalten. Je nach rechtlicher und technischer Einbindung solcher Dienste kann trotz der Anonymisierung von IP-Adresse und möglicherweise weiteren Daten zielgruppenspezifische Werbung ermöglicht werden, ohne dass der exakte Personenbezug den Werbenden oder von ihnen eingeschalteten Dienstleistern bekannt wird.

12.3 Fazit

Es gibt eine Reihe von Erfolg versprechenden Geschäftsmodellen, die auf dem Schwerpunkt Datenschutz fußen. Die Berücksichtigung von Datenschutzinteressen der Spieler und die Integration von Datenschutzmaßnahmen bietet, insbesondere den Herstellern, Publishern und Betreibern von Online-Spielen, die Möglichkeit, sich von Wettbewerbern positiv abzuheben und den Spielern vertrauensvoll am Markt entgegenzutreten.

Es ist nicht zu erwarten, dass das alleinige Angebot von Leistungen zu einer überwältigenden Nachfrage führt. Vielmehr sind eine fundierte Aufklärungsarbeit und Referenzkunden die beste Werbung. In einzelnen Branchen lässt sich beispielsweise beobachten, dass, sobald ein Unternehmen sich mit dem Datenschutz-Gütesiegel einen Wettbewerbsvorteil bei den Kunden „erarbeitet“ hat, konkurrierende Unternehmen mit der gleichen Zielgruppe nachziehen. Eine Zertifizierung eines Produktes führt zu einem Doppeleffekt. Zum einen hebt sich das Produkt besonders hervor, zum anderen geraten die Vergleichsprodukte der Mitbewerber unter Zugzwang, sich ebenfalls zum Umgang mit personenbezogenen Daten zu äußern und ihren Datenschutz zu verbessern. Es zahlt sich aber für ein Unternehmen aus, in diesem Bereich Vorreiter zu sein, um einerseits seinen Vorsprung gegenüber anderen Unternehmen auszubauen und die geeigneten Prozesse für die Verarbeitung personenbezogener Daten frühzeitig in die Unternehmensabläufe einzubinden und andererseits bei der Präsentation des Datenschutzthemas gegenüber den Kunden aus dem Feld der Mitbewerber rauszuragen.

Bei den entwickelten Geschäftsmodellen handelt es sich um idealtypische Modelle, die Platz für entsprechenden Gestaltungsraum bieten und somit weitere Geschäftsfelder eröffnen können. Der Online-Spielebereich zeichnet sich durch Innovativität und Kreativität aus. So ist damit zu rechnen, dass sich durch die datenschutzrechtlichen Anforderungen auch die Geschäftsmodelle für Datenschutz in Online-Spielen entsprechend weiterentwickeln werden und sich dadurch ein entsprechendes Betätigungsfeld für Fachleute bietet.

13 Ergebnisse und Forschungsbedarf

13.1 Ergebnisse und Handlungsempfehlungen der Studie

Die vorliegende Studie zeigt datenschutzrechtliche Vorgaben im Zusammenhang mit dem Angebot und der Nutzung von Online-Spielen auf. Da Online-Spiele auf Netzverbindungen beruhen, beziehen sich viele der rechtlichen Fragen auf den generellen Umgang mit dem Medium Internet. In ähnlicher Form stellen sie sich auch in Zusammenhang mit z. B. Service-orientierten Architekturen, Online-Shops, Sozialen Netzwerken und Suchmaschinen. In diesen Bereichen konnte die Studie die umfangreiche Problematik nur anreißen. Ein Schwerpunkt wurde auf die detaillierte Erörterung der für Online-Spiele besonders relevanten datenschutzrechtlichen Fragestellungen gelegt.

Um das Ziel eines datenschutzkonform gestalteten Online-Spiels zu erreichen, sind von den Spiele-Herstellern schon während der Entwicklungsphase die Datenschutzgrundsätze und rechtlichen Vorgaben zu berücksichtigen. In dieser Phase ist es möglich, die Systeme und Prozesse derartig zu gestalten, dass die Grundsätze der Datensparsamkeit und Datensicherheit beachtet und geeignet umgesetzt werden. Auch die Spiele-Betreiber bzw. die jeweils verantwortlichen Stellen für die Datenverarbeitung müssen in den einzelnen Phasen der Diensterbringung vom Vertrieb über Installation und Betrieb bis hin zur Kündigung die Verarbeitung die jeweilig anfallenden personenbezogenen Daten dahingehend hinterfragen, ob für den jeweiligen Fall eine Rechtsgrundlage vorhanden ist oder aber eine wirksame Einwilligung des Spielers vorliegt. Dabei ist auch jeweils zu untersuchen, welches Rechtssystem zur Anwendung kommt. In dieser Studie wurde der Schwerpunkt auf das deutsche Recht gelegt, das für die meisten Spiele, die in Deutschland angeboten werden, gilt oder zumindest vergleichbar zur Regelung in anderen EU-Staaten ist.

Unabhängig von der Rechtmäßigkeit der Erhebung, Verarbeitung oder Nutzung der jeweils anfallenden personenbezogenen Daten und der Einwilligung des Spielers sind von allen verantwortlichen Stellen die Grundsätze der Zweckbindung, Erforderlichkeit, Transparenz und Datensicherheit zu gewährleisten. Dies kann dadurch unterstützt werden, dass alle verantwortlichen Stellen ihre Dienste und Prozesse derartig dokumentieren, dass für alle Prozesse bestimmbar ist, welche personenbezogenen Daten auf welcher Rechtsgrundlage jeweils erhoben, verarbeitet und genutzt werden. Für jeden dieser Prozesse muss dann strukturiert untersucht werden, ob die erhobenen, verarbeiteten oder genutzten personenbezogenen Daten für den jeweiligen Zweck erforderlich sind. Zusätzlich ist jeweils zu hinterfragen, ob anonyme oder pseudonyme Daten für den jeweiligen Prozess ausreichend wären und damit sogar gesetzlich gefordert sind.

Umfragen und Gespräche mit Spiele-Herstellern, -Betreibern und Spielern haben ergeben, dass ein Interesse an datenschutzkonformen Spiellösungen besteht, diese aber kaum ausreichend umgesetzt werden, da es an Kenntnissen über Probleme und Lösungsmöglichkei-

ten mangelt. Aus diesem Grund wurde ein Leitfaden entwickelt, der insbesondere Betreibern und Herstellern von Online-Spielen eine erste Orientierung auf diesem Rechtsgebiet liefert. Dieser Leitfaden ist auch für Spieler interessant. Anhand der Aufzählungen kann von den Spielern selbst untersucht werden, ob sich das gespielte Spiel an die datenschutzrechtlichen Vorgaben hält.

Der Leitfaden als Ergebnis der Studie stellt die wichtigsten Funktionen in Online-Spielen dar und führt zu jeder dieser Funktionen die jeweiligen Rechtsgrundlagen für die Erhebung, Verarbeitung oder Nutzung der anfallenden personenbezogenen Daten auf. Weiterhin werden die wichtigsten datenschutzrechtlichen Probleme erörtert und mögliche Lösungen dargestellt.

Neben der Entwicklung des Leitfadens wurden Geschäftsmodelle für Hersteller und Betreiber von Online-Spielen aufgezeigt, die es den Spielern ermöglichen, sich über die Datenschutzkonformität eines Spiels zu informieren. Insbesondere die Möglichkeit Gütesiegel im Bereich des Datenschutzes für einzelne Produkte zu erhalten, kann auch zu einer verbesserten Akzeptanz auf dem deutschen Markt führen.

13.2 Forschungsbedarf

Zur datenschutzkonformen Gestaltung von Online-Spielen wurden 27 Funktionalitäten bzw. Module in Online-Spielen identifiziert, bei denen personenbezogene Daten der Spieler erhoben, verarbeitet oder genutzt werden. Diese Funktionalitäten enthalten nur die wesentlichen Funktionen der auf dem Markt befindlichen Online-Spiele. Sie sind aufgrund der sehr unterschiedlichen Spiele und Spielfunktionen für eine umfassende Handlungsempfehlung für Spielentwickler und -betreiber erweiterungsfähig und erweiterungsbedürftig. Insbesondere die neueren Entwicklungen im Rahmen der Einbindung von Online-Spielen in Soziale Netzwerke, die Steuerung von Online-Spielen ohne Eingabegeräte und die Erkennbarkeit von Personen in Online-Spielen werfen zusätzliche datenschutzrelevante Fragen auf.

Technisch-organisatorische Lösungen

Diese datenschutzrelevanten Fragen können teilweise schon im Bereich der technischen Entwicklungen und des Einsatzes neuer Technik gelöst werden. Es ist demnach erforderlich, technisch-organisatorische Maßnahmen für Online-Spiele nutzbar zu machen, um die allgemeinen Datenschutzgrundsätze, wie Datensparsamkeit und Datensicherheit, schon bei der Entwicklung von Online-Spielen berücksichtigen zu können. Es sind zusätzliche technische Möglichkeiten der Pseudonymisierung und Anonymisierung von personenbezogenen Daten in Online-Spielen zu untersuchen.

Transparenz

Weiterhin sollten die Möglichkeiten untersucht werden, wie für Online-Spieler Transparenz in Bezug auf die Verarbeitung ihrer personenbezogenen Daten geschaffen werden kann. Insoweit ist zu prüfen, inwieweit die Spieler selbst umfassenden Einblick in die Datenerhebung, -verarbeitung und -nutzung erhalten können. Dies muss insbesondere personenbezogene Daten und Bereiche betreffen, in denen sich die Spieler nur selten bewusst darüber sind,

dass Daten erhoben, verarbeitet oder genutzt werden. Hier könnten Lösungen erörtert werden, die den Spielern die personenbezogenen Daten sichtbar machen.

Einbeziehung Dritter

Auch sollten Funktionalitäten, die durch Dritte bereitgestellt werden, auf ihre Datenschutzkonformität überprüft werden und nur datenschutzgerechte Produkte eingesetzt werden. Diese Produkte bedürfen jedoch einer weitergehenden Untersuchung und der Prüfung einer datenschutzgerechten Einbindung in die Online-Spiele. In diesem Zusammenhang könnten vor allem Produkte mit anerkannten Datenschutz-Gütesiegeln eingesetzt werden.

Neue Entwicklungen in Online-Spielen

Neben diesem während der Studie identifizierten zusätzlichen Untersuchungsbedarf, sind zum Ende des Untersuchungszeitraums weitere datenschutzrelevante Fragen aufgetreten, die einer weiterführenden Untersuchung bedürfen. Zum einen werden Online-Spiele vermehrt in Soziale Netzwerke integriert, was dazu führt, dass die in den sozialen Netzwerken vorhandenen personenbezogenen Daten in die Spiele und den Spielablauf integriert werden. So ist es möglich, dass Spieler ihre Kontaktdaten und Kontakte auch für andere Spieler freigeben und so ein umfassender, nahezu intransparenter Datenfluss entsteht. Durch die Integration neuartiger Sensoren in das Spielgeschehen, wie Kinect und Schrittzähler, werden sensible personenbezogene Daten, wie Gesundheitsdaten oder Konstitutionsdaten, in den Spielbetrieb integriert und teilweise allgemein zugänglich gemacht. Auch die Einbeziehung von Geodaten in Online-Spiele auf mobilen „Spielgeräten“ kann zu der Entstehung eines Bewegungsprofils eines Spielers führen und damit neue datenschutzrechtliche Probleme aufwerfen (vgl. Abschnitt 3.4).

Rechtliche Entwicklungen

In einer weitergehenden Analyse von neuen Entwicklungen und dem Aufzeigen von datenschutzkonformen Lösungsmöglichkeiten sind auch die rechtlichen Änderungen zu berücksichtigen.

So entscheidet sich 2010 / 2011 die Entwicklung der Vorratsdatenspeicherung für Telekommunikationsdiensteanbieter, nachdem am 2. März 2010 das Bundesverfassungsgericht die ursprüngliche Regelung für nichtig erklärt hat.

Noch Ende 2009 erschien die „Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz“. Diese muss nunmehr in nationales Recht umgesetzt werden und enthält Änderungen u. a. zur Mitteilungspflicht bei Datenpannen und dem Umgang mit Cookies.

Abkürzungsverzeichnis

§	Paragraf
§§	Paragrafen
3D	dreidimensional
Abb.	Abbildung
Abo.	Abonnement
Abs.	Absatz
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
Art.	Artikel
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Apps	Applications
Az.	Aktenzeichen
B2C	Business-to-Consumer
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BDSG	Bundesdatenschutzgesetz
Bsp.	Beispiel
bzw.	beziehungsweise
d.h.	das heißt
DoS	Denial of Service
DOS	Datenschutz in Online-Spielen
DRM	Digital Rights Management
DSE	Datenschutzerklärung
DSL	Digital Subscriber Line
DSVO	Datenschutzverodnung
DVD	Digital Video Disc
EG	Europäische Gemeinschaft
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
E-Mail	Electronic Mail
EMRK	Europäische Menschenrechtskonvention
ESA	European Space Agency

Etc.	et cetera
EU	Europäische Union
EULA	Endbenutzerlizenzvertrag
EuroPriSe	European Privacy Seal
EUV	Vertrag über die Europäische Union
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	fortfolgende
FPS	First Person Shooter
ggf.	gegebenenfalls
HGB	Handelsgesetzbuch
ID	Identifikation, Identifikationsnummer
IP	Internet Protocol
i. S. d.	im Sinne der/des
IT	Informationstechnik
i. V. m.	in Verbindung mit
JMStV	Jugendmedienschutz-Staatsvertrag
JuSchG	Jugendschutzgesetz
KPI	Key Performance Indikator
KunstUrhG	Kunsturhebergesetz
LAN	Local Area Network
lit.	Litera
Mio.	Million(en)
MMOG	Massively Multiplayer Online Game (Massen-Mehrspieler-Online-Gemeinschaftsspiel)
MMORPG	Massively Multiplayer Online Role-Playing Game (Massen-Mehrspieler-Online-Rollenspiel)
Mrd.	Milliarde(n)
NDS	Nintendo DS
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
o. g.	oben genannt
PC	Personal Computer
PersAuswG	Personalausweisgesetz
PS 1	PlayStation 1
PS 2	PlayStation 2
PS 3	PlayStation 3

PSN	PlayStation Network
PSP	PlayStation Portable
sog.	so genannt
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u. a.	unter anderem
u. ä.	und ähnlich
ULD	Unabhängiges Landezentrum für Datenschutz Schlesig-Holstein
UN	United Nations
US	United States
USA	United States of America
USK	Unterhaltungssoftware Selbstkontrolle
VG	Verwaltungsgericht
vgl.	vergleiche
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WPA	Windows Product Activation
z. B.	zum Beispiel

Literaturverzeichnis

Bäumler, Helmut	Marktwirtschaftlicher Datenschutz, in: DuD – Datenschutz und Datensicherheit 06/2002, S. 325-329.
Bizer, Johann	Sieben Goldene Regeln des Datenschutzes, in: DuD 2007, S. 350 ff.
Bizer, Johann	Datenschutz in die Prozesse, in: DuD 10/2006, S. 598.
BITKOM / Deloitte	Spielend unterhalten – Wachstumsmarkt Electronic Games – Perspektive Deutschland.
Bock, Kirsten	EuroPriSe – Das Datenschutz-Gütesiegel aus Schleswig-Holstein wird europäisch, in: DuD 06/2007, S. 410.
Borchers, Detlef	Datenschutzmanagement als Wettbewerbsfaktor in IT-Sicherheit & Datenschutz 11/2006, S. 721-724.
Buron, Marie-Anne	Frankreich: Klare Regeln für Computerspiele gefordert, in: MMR 2008, S. XVIII.
Büllesbach, Alfred	Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsvorteil, in: RDV 1997, 239 ff.
Couper, Mick P. / Coutts, Elisabeth	Online-Befragung. Probleme und Chancen verschiedener Arten von Online-Erhebungen, in Diekmann, Andreas, Methoden der Sozialforschung, Kölner Zeitschrift für Soziologie und Sozialpsychologie, Sonderheft 44/2004, 2006, S. 217-243.
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.)	Bundesdatenschutzgesetz Kompaktkommentar, Frankfurt am Main, 3. Auflage 2010.
Diekmann, Andreas	Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen, 1995, Hamburg.
ENISA	Survey Results – Security And Privacy In Massively-Multiplayer Online Games And Social And Corporate Virtual Worlds, 2008.
ENISA	Virtual Worlds, Real Money, 2008.
ESA	Sales, Demographic and Usage Data. Essential Facts about the Computer and Video Game Industry, 2008.

Ferguson, Christopher John	The Good, The Bad and the Ugly: A Meta-analytic Review of Positive and Negative Effects of Violent Video Games, in: Psychiatric Quarterly 78 (4), 2007, S. 309-316.
Fraunhofer-Institut für Digitale Medientechnologie / Unabhängigen Landeszentrum für Datenschutz / Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau	Datenschutzverträgliches und nutzerfreundliches Digital Rights Management – Privacy4DRM, Studie im Auftrag des Bundesministerium für Bildung und Forschung; 2005.
Geis, Ivo / Geis, Esther	Rechtsaspekte des virtuellen Lebens, in: CR 2007, S. 721 ff.
Gola, Peter / Schomerus, Rudolf	BDSG Bundesdatenschutzgesetz, München, 9. Auflage 2007.
Griffiths, Mark D. / Mark N.O. Davies / Darren Chappell	Breaking the Stereotype: The Case of Online Gaming, in: Cyberpsychology & Behavior 6(1), 2003, S. 81-91.
Griffiths, Mark D. / Mark N.O. Davies / Darren Chappell	Demographic Factors and Playing Variables in Online Computer Gaming, in: Cyberpsychology & Behavior 7(4), 2004, S. 479-487.
Habel, Oliver M.	Eine Welt ist nicht genug – Virtuelle Welten im Rechtsleben, in: MMR 2008, S. 71 ff.
Heckmann, Dirk	juris Praxiskommentar Internetrecht, Saarbrücken, 2007.
Hoeren, Thomas / Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht, München, 21. Ergänzungslieferung 2008.
Holsapple, Clyde W. / Wu, Jiming	Building effective online game websites with knowledge-based trust, in: Information Systems Frontiers 10(1), 2008, S. 47-60.
Hopf, Kristina	Rechtliche Grundlagen des Jugendmedienschutz-Staatsvertrags und die Verantwortlichkeit von Chatbetreibern, in: ZUM 2008, S. 207.
Institut für Demoskopie Allensbach	Zu wenig Datenschutz? Die meisten sind mit persönlichen Daten vorsichtig geworden. Allensbacher Bericht Nr. 6/2009.
Jansz, Jeroen / Tanis, Martin	Appeal of Playing Online First Person Shooter Games, in: Cyberpsychology & Behavior 10(1), 2007, S. 133-136.

Jöckel, Sven	Online Spiele – Eine konzeptuelle Abgrenzung verschiedener Spielformen, in: Technische Universität Ilmenau, Menschen, Märkte, Medien Management – Berichte aus Forschung und Lehre 02/2007.
Jotzo, Florian	Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, S. 232 ff.
Kimmert, Christoph	Computer- und Videospiele in: Mangold, Roland / Vorderer, Peter / Bente, Gary, Lehrbuch der Medienpsychologie, S. 695-716.
Koch, Pamela	Die rechtliche Bewertung virtueller Gegenstände auf Online-Plattformen, http://www.jurpc.de/aufsatz/20060057.htm.
Koos, Stefan	Der Name als Immaterialgut, in: GRUR 2004, S. 808 ff.
Krasemann, Henry	Identitäten in Online-Spielen, in: DUD 2008, S. 194 ff.
Leisner, Walter	Das neue „Kommunikationsgrundrecht" – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung, in: NJW 2008, S. 2902 ff.
Logistik Heute	Spiele Picken, in: Logistik Heute 6/2009, S. 20-21.
Meints, Martin	Datenschutz durch Prozesse, in: DuD 02/2007, S. 91-95.
Meissner, Sebastian	Zertifizierungskriterien für das Datenschutzgütesiegel EuroPriSe, in: DuD 08/2008, S. 525-531.
Pötzsch, Stefanie	Privacy Awareness – A Means to Solve the Privacy Paradox?, in: The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Vol. 298, Springer 2009, S. 226-236.
Ponemon Institute	Airport Insecurity: The Case of Lost & Missing Laptops, Juli 2008.
Ponemon Institute	Fourth Annual US Cost of Data Breach Study, Januar 2009.
Rebmann, Kurt / Säcker, Franz Jürgen / Rixecker, Roland (Hrsg.)	Münchner Kommentar, München, 5. Auflage 2006, Band 1.
Roßnagel, Alexander	Die Novellen zum Datenschutzrecht – Scoring und Adresshandel, in: NJW 2009, S. 2716 ff.
Roßnagel, Alexander	Das Telemediengesetz Neuordnung für Informations- und Kommunikationsdienste, in: NVwZ 2007, S. 743 ff.

Rost, Martin	Welches Gesetz gilt eigentlich?, https://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm/.
Rost, Martin / Pfitzmann, Andreas	Datenschutz-Schutzziele – revisited, in: DuD 06/2009, S. 353-358.
Schaar, Oliver	In-Game-Advertising, in: CR 2006, S. 619 ff.
Scheja, Gregor	Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, Baden-Baden, 2005.
Schläger, Uwe	Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein, in: DuD 08/2004, S. 459-461.
Schleipfer, Stefan	Das 3-Schichtenmodell des Multimediadatenschutzrechts, in: DuD 2004, S. 727 ff.
Schnell, Rainer / Hill, Paul B. / Esser, Elke	Methoden der empirischen Sozialforschung. 7. völlig überarbeitete und erweiterte Auflage. München: Oldenburg, 2005.
Schulze, Victoria / Jöckel, Sven / Will, Andreas	Grundlagen der Werbewirkungsforschung für Ingame-Advertising, in: Menschen Märkte Medien Management – Berichte aus Forschung und Lehre 01/2007, TU Ilmenau.
Simitis, Spiros (Hrsg.),	Bundesdatenschutzgesetz Kommentar, Baden-Baden, 6. Auflage 2006.
Sozioland	Games-Umfrage 2008, 2008.
Spiekermann, Sarah / Grossklags, Jens / Berendt, Bettina	E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, in: Proceedings of the 3rd ACM Conference on Electronic Commerce, New York, 2001, S. 28-47
Spindler, Gerald/Schuster, Fabian (Hrsg.)	Recht der elektronischen Medien, München, 2008.
Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer W.	Einführung in das Datenschutzrecht, München, 4. Auflage 2005.
Unabhängiges Landeszentrum für Datenschutz / Institut für Informatik der Universität Koblenz-Landau/ Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau	SOAinVO – Chancen und Risiken von Service-orientierten Architekturen in Virtuellen Organisationen, 2007.

Unabhängiges Landeszentrum für Datenschutz / Technische Universität Dresden	Verkettung digitaler Identitäten, Report im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel, 2007.
Weichert, Thilo	Datenschutzberatung – Hilfe zur Selbsthilfe in Helmut Bäumler (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 213 ff.
Williams, Dmitri / Yee, Nick / Caplan, Scott E.	Who plays, how much, and why? Debunking the stereotypical gamer profile, in Journal of Computer-Mediated Communication 13(X), 2008, S. 993-1018.
Wood, Richard T.A. / Griffiths, Mark D. / Eatough, Virginia	Online Data Collection from Video Game Players: Methodological Issues, in: Cyberpsychology & Behavior 7(5), 2004, S. 511-518.
Wu, Jiming / Liu, De	The effects of trust and enjoyment on intention to play online games, in: Journal of Electronic Commerce Research 8(2), 2007, S. 128-140.
Yee, Nick	The Demographics, Motivations and Derived Experiences of Users of Massively-Multiuser Online Graphical Environments, in: PRESENCE: Teleoperators and Virtual Environments 15(3), 2006, S. 309-332.

Dokumente

Bundesgerichtshof	BGH, Urteil vom 30. März 2006, Az.: I ZR 24/03, BGHZ 167, S. 91 ff.
Bundestag	BT-Drs. 16/3078, S. 15 Gesetzesbegründung zum TMG
Bundestag	BT-Drs. 16/13657, S. 33
Bundestag	BT-Drs. 14/ 4329, S. 31 f. Regierungsentwurf zum BDSG
Bundesverfassungsgericht	BVerfGE 65, S. 1 ff.
Bundesverfassungsgericht	BVerfG NJW 2008, S. 822
Düsseldorfer Kreis	Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung der Fallgruppen zur internationalen Auftragsdatenverarbeitung, S. 16
EuGH	Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971 ff.
EuGH	Rs. C-275/06 (Promusicae), Slg. 2008, S. I-271 ff.

EuGH	Rs. C-208/00 (Überseering BV./.Nordic Construction Company Baumanagement GmbH), Slg. 2002, S. I-9919 ff.
EWR	Anhang XI 5e.01 zur EWR-Rechtssammlung 6. November 2009, http://www.llv.li/pdf-llv-sewr-ewr_register.pdf
OECD Declaration on Transborder Data Flows	The OECD Observer, Nr. 135
Richtlinie 2002/58/EG	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 vom 31.07.2002, S. 37-47
Richtlinie 2006/24/EG	Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EG Nr. L 105 vom 13.04.2006, S. 54-63
Richtlinie 2007/65/	Richtlinie 2007/65/EG des Europäischen Parlaments und des Rates vom 11.12.2007 zur Änderung der Richtlinie 89/552/EWG des Rates zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Ausübung der Fernsehtätigkeit, ABl. EG Nr. L 332 vom 18.12.2007, S. 27 (29)
Richtlinie 95/46/EG	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABL. EG Nr. L 281 vom 23.11.1995, S. 31-50
Richtlinie 97/66/EG	Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG Nr. L 24 vom 30.01.1998, S. 1-8
UN Resolution 45/95	http://www.un.org/documents/ga/res/45/a45r095.htm