Bundesministerium
für Bildung
und Forschung

DOS

Datenschutz in Online-Spielen

Studie im Auftrag des BMBF

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

DOS – Datenschutz in Online-Spielen

Leitfaden
für Hersteller, Publisher und Betreiber von Online-Spielen

Stand: 14. September 2010

Im Auftrag des Bundesministeriums für Bildung und Forschung

Die gesamte Studie finden Sie unter:
http://www.datenschutzzentrum.de/dos

Verfasser:
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, 24103 Kiel
Tel: 0431 988 - 1398
mail@datenschutzzentrum.de

Inhaltsverzeichnis

I. Einleitung **3**
II. Datenschutzrelevante Funktionen in Online-Spielen **5**
1. Generelle Vorkehrungen 5
2. Vertrieb 9
3. Installation und Registrierung 11
4. Betrieb und Überprüfung 13
5. Bezahlsystem 15
6. Kündigung / Spielbeendigung 17
7. Spieler-zu-Spieler-Erkennbarkeit 19
8. Reputationssystem / Beschwerdemanagement 20
9. Highscoreliste 22
10. Ligamodus 23
11. Eigenpräsentation des Spielers 25
12. Upload 26
13. Chat 27
14. Nachrichtenaustausch 29
15. Datenschutzkonfiguration 32
16. Datenschutzerklärung 33
17. Weiterleitung von Daten an Dritte 35
18. In-Game-Advertising 37
19. Altersverifikation und Jugendschutz 39
20. Suchtprävention 40
21. (In-Game-)Shopping 41
22. In-Game-Verhaltensanalyse 42
23. Webcam / Videoaufzeichnung 44
24. Always-Online-Funktionalität 46
25. Mobile-Gaming 47
26. Spielen über Internet 49
27. Einbindung in Soziale Netzwerke 51

I. 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 Bundesdatenschutzgesetz (BDSG)). Soweit das Telekommunikations-gesetz (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 Telemediengesetz (TMG). Sofern der Spiele-Betreiber zumindest eine Niederlassung in Deutschland hat, sind die hier großenteils relevanten 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).

II. Datenschutzrelevante Funktionen in Online-Spielen

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[1] / EuroPriSe[2]).
- 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 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.

---

1 https://www.datenschutzzentrum.de/guetesiegel/index.htm.

2 https://www.european-privacy-seal.eu/.

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.

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 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 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/.

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 (vgl. Abschnitt 16).

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 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.

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 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.

5. Bezahlsystem

a) Funktionalitätsbeschreibung

Über den Vertrieb des Spiels (vgl. Abschnitt 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 (vgl. Studie 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.

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

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.

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

werden. 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. 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.

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.

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.

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.

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 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 (vgl. Abschnitt 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 (Zeitschrift für Urheber- und Medienrecht (ZUM) 2008, S. 207).

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 4)

Für Anbieter der elektronischen Post galt bis zum Urteil des Bundesverfassungsgerichts vom 2. März 2010[3] 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

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

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.

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.

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.

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 Nutzer 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.

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.

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 Gesundheits-

zustand 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.

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.

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.

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 besteht. 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.

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.

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. Jugendliche, 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 (vgl. Abschnitt 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.

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.

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.

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 (vgl. Abschnitt 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.

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.