Datenschutz in Spielen

EIN DATENSCHATZ ZUM ZUGREIFEN

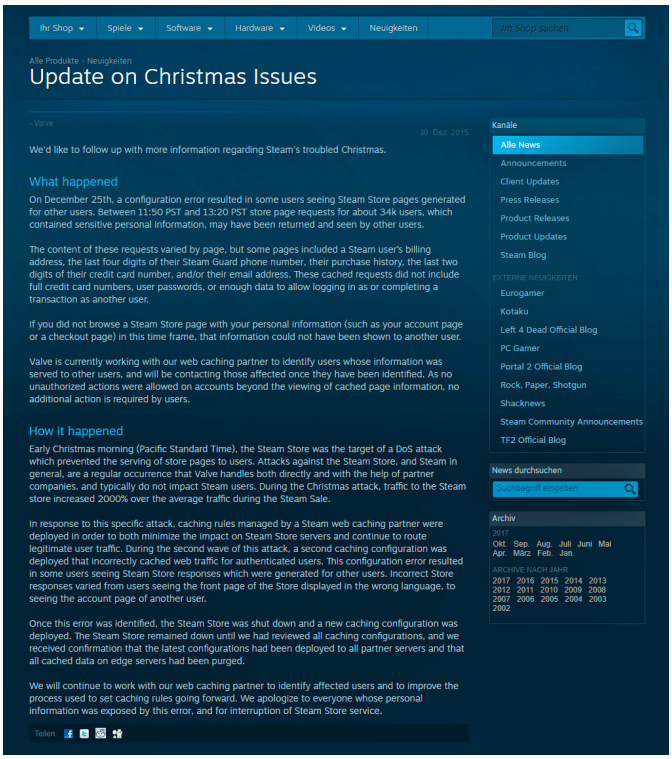
Spieler produzieren im Laufe ihres interaktiven Daseins viele, viele Daten. Datenschutz sollte absolute Priorität haben, wenn man sich online einloggt. Doch dafür interessieren sich scheinbar nur wenige Spieler und noch weniger Unternehmen. Also gehen Hersteller munter auf Daten-Sammeljagd – doch ein neues EU-Gesetz könnte der Goldgräberstimmung ein Ende setzen. Von Martin Dietrich

Wir reißen die Verpackung des sehnlichst erwarteten Spiels auf und werfen die DVD hastig ins Lesegerät. Bevor der Installer seinen lebenswichtigen Dienst verrichtet und die geforderten Daten auf die Festplatte schaufelt, müssen wir uns jedoch erst auf einer Online-Plattform anmelden. Als erfahrener Videospieler kennen wir das Prozedere mittlerweile. Ein paar Klicks später ist die Software auf unserem Rechner und die Anmeldedaten sind in alle geforderten Felder eingetippt. Nur ein Häkchen trennt uns noch vom sorgenlosen Spielvergnügen: die Datenschutz-Richtlinie. Klar, die haben wir gelesen, verstanden und akzeptiert. Gut, zumindest Letzteres trifft zu, denn so richtig beschäftigen wollen wir uns damit nicht. Schließlich hätte ein »Nein« auch ein »Nein« seitens der Online-Plattform zur Folge – und das Spiel liefe nicht. Und was will so eine Online-Plattform denn schon von uns wissen? Eine ganze Menge.

Interessant ist erst mal alles

Werfen wir doch mal einen Blick auf das Textmonster namens Datenschutz-Richtlinie. Man wolle »Verhaltensmuster und Gewohnheiten der Nutzer« auswerten, heißt es bei Steam, und Origin hat ein Interesse an Leistungen, Benutzerranglisten, der Zeit, die wir für Spiele aufwenden, und an Klickpfaden. Dazu kommen oft noch unser Name, Adressdaten, Geburtsdatum und teilweise welche Hard-und Software von Drittherstellern auf dem PC installiert sind. Firmen wie Valve, Electronic Arts oder Ubisoft häufen einen gewaltigen Datenschatz an, den sie zu unlauteren Zwecken missbrauchen könnten. Oder sie werden zum Opfer der eigenen Schludrigkeit, wenn sie diese Informationen nicht ausreichend schützen. So werden im Januar 2015 1.800 Minecraft-Benutzernamen mitsamt Passwörtern ausspioniert und veröffentlicht. Im gleichen Jahr können Steam-Nutzer auf-

Auch Minecraft war schon Ziel von Hackerangriffen. 2015 wurden rund 1.800 Accounts geklaut – wohlgemerkt bei einem Spiel, das häufig von Minderjährigen gespielt wird.



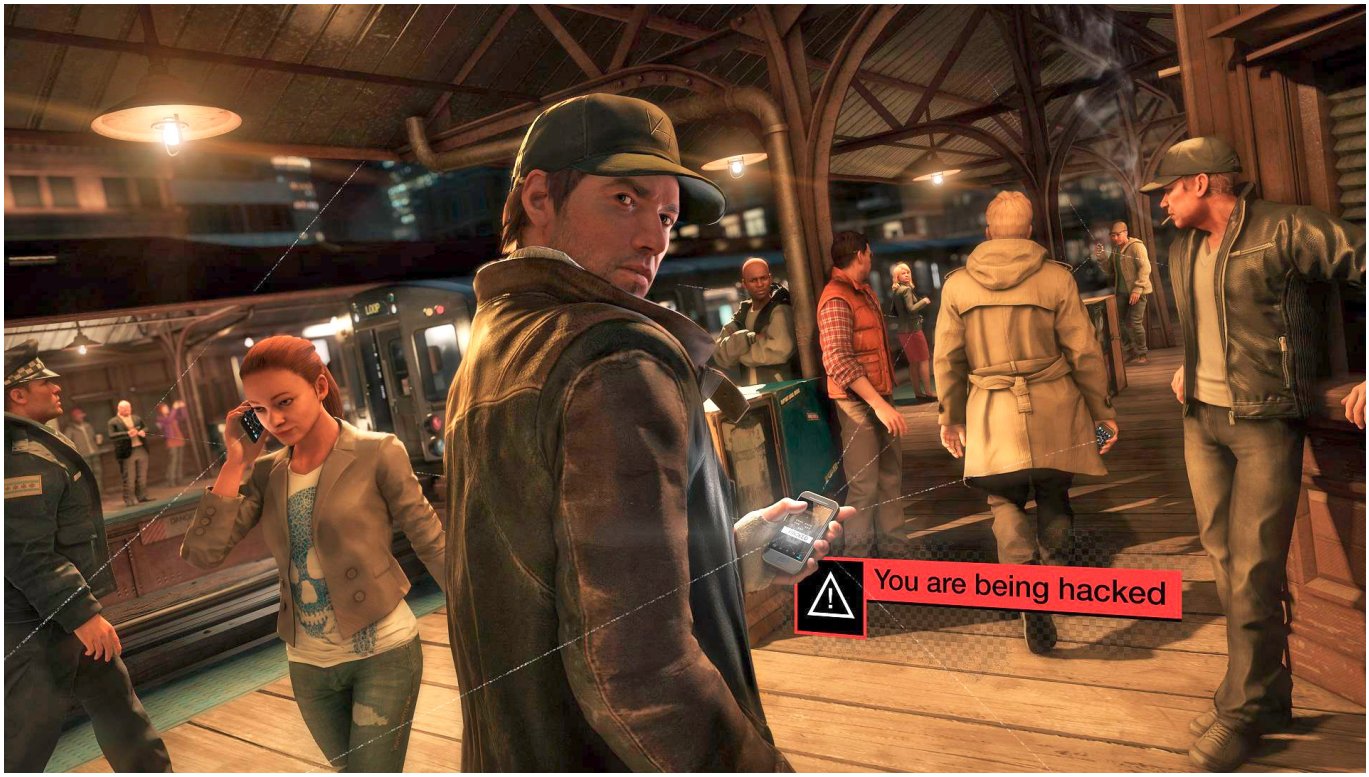
Aufgrund eines Caching-Fehlers können Steam-Nutzer an Weihnachten 2015 teilweise sensible Informationen anderer Accounts einsehen, darunter E-Mail-Adressen oder Telefonnummern. Erst fünf Tage später gesteht Valve den Vorfall in einem Blogbeitrag ein.

grund eines internen Speicherfehlers zeitweise sensible Daten anderer Accounts einsehen, etwa die letzten Ziffern der Kreditkarte oder die Telefonnummer. Noch schlimmer trifft es 2011 Sony, als ein Hackerangriff auf ihr PlayStation-Ökosystem rund 77 Millionen Accounts vogelfrei macht. Die Enthüllungen des Whistleblowers Edward Snowden offenbaren überdies, dass der amerikanische Geheimdienst NSA Chats in World of Warcraft oder Second Life überwachen ließ. Laut den Enthüllungen wurden bei Second Life an drei Tagen mehr als 170.000 Zeilen an Nachrichten gesammelt und ausgewertet.

Kurz bevor Electronic Arts 2011 den Online-Shooter Battlefield 3 veröffentlichte, startete der Publisher auch seinen bisherigen Download-Manager als Steam-Konkurrent neu und benannte ihn in Origin um. Doch in dessen Nutzungsbedingungen verbargen sich allerlei rechtlich fragwürdige oder gar direkt unzulässige Klauseln. Beispielsweise sicherte sich EA in einer frühen Version der Lizenzvereinbarung (End User License Agreement, EULA) das Recht, personenbezogene Daten wie Namen und Adressen auszulesen und sogar zu Marketingzwecken zu verwenden. Als wir diese und andere Verstöße in einem GameStar-Artikel brandmarken, erhebt sich vor allem in Deutschland ein Aufschrei gegen die Datenkrake Origin – mit über drei Millionen Seitenaufrufen ist dieser Artikel bis heute der meistgelesene der GameStar-Geschichte. Nach einer Protestwelle weicht EA den Datenschutztext auf und verspricht Zurückhaltung. Echte Strafen hätte der Publisher jedoch nicht fürchten müssen, denn eine zahnlose Rechtsprechung und konstruierte Verträge stehen den Datensammlern kaum im Wege. Und das, obwohl die Gesetzgebung strenge Regeln aufstellt.

Entstanden aus einer Klagewelle

In Deutschland rückt das Thema Datenschutz erstmals im Jahr 1983 ins Zentrum der öffentlichen Aufmerksamkeit und wird heiß diskutiert. Im Rahmen einer Volkszählung sammelt der Staat zu dieser Zeit große Datenmengen von den Bürgerinnen und Bürgern. Als sich Bedenken häufen, was der Bund mit den Adressdaten anstellen könnte, und immer mehr Bürger gegen die Volkszählung klagen, ersinnt das Bundesverfassungsgericht die Idee der sogenannten informationellen Selbstbestimmung. »Das Verfassungsgericht sagte, wenn die Würde des Menschen unantastbar sei und die Freiheit des Menschen durch den Staat nicht eingeschränkt werden solle, dann folge daraus, dass jeder Bürger grundsätzlich selbst bestimmen soll, was mit seinen Daten passiert. Daraus ist dann der Datenschutz entwickelt worden«, erklärt der Rechtsanwalt Kai Bodensiek die Geschichte hinter dem Begriff informationelle Selbstbestimmung. Die drei



Ubisoft veröffentlichte 2012 versehentlich zahlreiche E-Mail-Adressen privater Spieler von Watch Dogs, die den Newsletter abonniert hatten – die Sammelmail enthielt alle Adressen im Klartext. Reinste Ironie, wenn man das Überwachungssetting von Watch Dogs bedenkt.

wichtigsten Gesetze, die Datenschutz zwischen Verbrauchern und Firmen in Deutschland betreffen, sind das Bundesdatenschutzgesetz, das Telemediengesetz und das Telekommunikationsgesetz. Darin werden die Rechte der Verbraucher und die Möglichkeiten zur Beschwerde aufgelistet. Die Gesetzestexte decken dabei nur personenbezogene Daten ab, die auf eine einzelne Person konkret oder auch nur mittelbar schließen lassen. Darunter fallen insbesondere Namen, Adressen, Überweisungsdaten und andere Persönlichkeitseigenschaften. Sind Daten vollständig anonymisiert oder zu unspezifisch, um einen einzelnen Menschen zu identifizieren, fallen sie unter keinerlei staatliche Regulierung oder Einschränkung.

Keine Selbstverständlichkeit

Die meisten Daten, die Steam, Origin und Co. sammeln, gelten jedoch als personenbezogen: Adressen, Namen, Kreditkartennummern. Wer solche Daten speichern und verarbeiten will, muss in Deutschland hohe Hürden überwinden, erläutert der Jurist Henry Krasemann vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein: »Da gilt der Grundsatz bei uns, dass erst mal alles verboten ist. Es sei denn, man findet ein entsprechendes Gesetz oder hat die Einwilligung des Betroffenen, der die Datenverarbeitung wiederum zulässig macht.« So dürfen Unternehmen Daten auch zum Zwecke der Erfüllung eines Vertrages sammeln, also wenn die Firma die Daten benötigt, um ihren versprochenen und oft auch kostenpflichtigen Dienst ordnungsgemäß zu erfüllen. Wer etwa ein Zeitschriftenabonnement anbietet, muss den Namen und die Adresse des Abonnenten kennen und speichern. Falls die Interessen des Verwerters gegenüber dem Betroffenen deutlich überwiegen sollten, ist es ebenfalls meist zulässig, Daten zu sammeln. Diese Option ist jedoch komplizierter, bedarf einer juristischen Einschätzung und läuft laut Kai Bodensiek auf »eine Einzelfallabwägung« hinaus – das heißt, dass für jede Plattform ein eigenes Gerichtsurteil notwendig wäre. Insgesamt lässt sich das Datenschutzrecht jedoch auf eine einfache Regelung destillieren: Alles, was über das erwartbare Maß hinausgeht, benötigt eine explizite Erlaubnis des Nutzers. Das bedeutet, sobald Steam oder Uplay mehr Daten sammeln, als sie zur Instandhaltung ihre Server und der Abwicklung von Einkäufen brauchen, ist eigentlich eine gesonderte Einwilligung vonnöten.

Als Betroffener stattet einen die Gesetzeslage außerdem mit einigen Rechten aus, die man gegenüber der datensammelnden Firma besitzt. Egal, ob Daten ohne Kenntnis des Betroffenen oder auf der Grundlage einer Einwilligung verarbeitet werden: Diese Erlaubnis kann jederzeit zurückgezogen werden. Dann müssen auch die Daten gelöscht werden. Besteht ein anderer Grund für die Datensammlung, beispielsweise der Verdacht einer Straftat, ist es möglich, die Daten für jeden anderen Zweck

zu sperren. Außerdem besitzt jeder Bürger ein in der Regel kostenloses Auskunftsrecht, sodass er von Unternehmen verlangen kann, darüber informiert zu werden, wo die gespeicherten Daten liegen, und dass sie berichtigt werden, falls sie nicht stimmen. »Auskunft, Löschung, Berichtigung und Sperrung sind die wichtigen Rechte, die man als Verbraucher hat«, fasst Kai Bodensiek die Rechtslage zusammen. Dieses Bündeln aus Pflichten und Rechten basiert mittlerweile zu großen Teilen auf den Datenschutzvorgaben der Europäischen Union und gilt in Teilen auch in anderen EU-Ländern.

Verbraucherschutzverbände wie der Verein Digitalcourage aus Bielefeld setzten sich dafür ein, dass Unternehmen transparenter kommunizieren, was mit den Daten ihrer Kunden passiert. (Bild: Torben Meyer)

Macht doch einfach, was ihr wollt

Trotz dieser vielen Einschränkungen müssen allerdings auch deutsche Spieler viele lasche Datenschutzbedingungen lesen und akzeptieren, wenn sie die entsprechenden Dienste nutzen möchten. Das liegt zum einen an geringen Strafen – bei Verstößen droht Unternehmen bisher maximal eine Geldstrafe von 300.000 Euro, für Milliardenkonzerne ein Griff in die Portokasse. Bis eine Klage auch wirklich vor Gericht landet und ein Richter sein Urteil fällt, dauert es zudem oft mehrere Monate oder gar Jahre. Bis dahin haben sich meistens die Datenschutztexte schon dreimal wieder geändert und der technische Fortschritt verlangt abermals einen angepassten Gesetzestext.

»Schaut man sich dann die Datenschutzbedingungen im Detail an, dann bleiben meistens viele Fragen offen«, bestätigt Jurist Henry Krasemann. »Das sind Texte, die mit sehr vielen Platzhaltern arbeiten und mit irgendwelchen Unbestimmtheiten.« Gerade die Vereinigten Staaten haben im Gegensatz zu Deutschland einen weit weniger restriktiven Datenschutz und erlauben einen viel größeren Spielraum. Steam gibt beispielsweise an, bei automatisch erstellten Fehlerberichten, »gegebenenfalls auch Informationen über andere Software oder Hardware« zu sammeln. Blizzard wiederum verwendet die gesammelten persönlichen Daten »unter Umständen« auch für Marketingzwecke. »Sie halten meistens nicht dem Stand, was sich Aufsichtsbehörden als wirksame Einwilligung oder als wirksame Datenschutzerklärung vorstellen«, urteilt Krasemann mit Blick auf die oft schwammigen Texte der Publisher und Entwickler. Eine weitere Schwierigkeit stellt die räumliche Distanz zwischen dem datenverarbeitenden Server und der betroffenen Person dar. So landen die meisten Daten früher oder später auf US-amerikanischen Servern. »Aus europäischer Sicht darf man keine Daten in Ländern verarbeiten, die nicht dem europäischen Datenschutzniveau entsprechen, und dazu gehören auch die USA«, erklärt Jurist Henry Krasemann. Um diese Regelung zu umgehen, wurde ursprünglich das Safe-Harbor-Abkommen ins Leben gerufen. Unternehmen aus Übersee versprachen, sich ans europäische Datenschutzniveau zu halten. Allerdings reichte hierfür ein bloßes Lippenbekenntnis. Kontrollen seitens der EU oder gar Sanktionen gab es nicht. Diese Schwäche erkannte auch der Europäische Gerichtshof, der das Safe-Harbor-Abkommen 2015 für nichtig erklärte. An dessen Stelle trat Privacy Shield, das nach ähnlichen Prinzipien funktioniert, aber eine leichtere Beschwerdemöglichkeit für EU-Bürger bieten soll und US-Firmen verpflichtet, Daten zu löschen, wenn der Verwendungszweck entfällt.

Kritiker wie Krasemann sehen jedoch im Großen und Ganzen dieselben Probleme und vermuten, dass europäische Gerichte das Abkommen ebenfalls kippen könnten: »Das ganze Konstrukt ist nach meiner Einschätzung wieder sehr wackelig.« Erst recht, nachdem US-Präsident Donald Trump im Januar 2017 angeordnet hat, dass der Privacy Act nur für US-Staatsangehörige gelten soll. Dieses Gesetz von 1974 regelt, dass US-Behörden Einsicht in die von ihnen gespeicherten Daten geben müssen und diese auch nur mit Zustimmung der jeweiligen Person oder nach einem Gerichtsbeschluss weitergeben dürfen. Wenn schon der Staat nur US-Amerikanern dieses Minimum an Datenschutz zusichert, dürften sich Privatunternehmen noch viel weniger verpflichtet fühlen, Europäern Auskünfte zu erteilen oder gar Daten zu löschen. Im asiatischen Raum existiert nicht mal ein generelles Datenschutzabkommen. Europa schließt hier meistens einzelne Verträge mit Nintendo oder Sony, die ähnliche Probleme wie Privacy Shield aufweisen: Lippenbekenntnisse, aber wenig Kontrolle.

ELECTRONIC ARTS DATENSCHUTZRICHTLINIEN

Gültig ab: 25. Januar 2011

Durch Ihre Registrierung eines Electronic Arts (EA)-Kontos, durch die Nutzung dieser Website und/oder eines Online- oder Mobil-Produktes und -Dienstes von EA stimmen Sie den EA-Datenschutzrichtlinien zu und erlauben uns, Ihre Kontoangaben in die USA zu übermitteln und dort zu speichern. Durch die Registrierung stimmen Sie zu, dass EA Ihre Daten gemäß den folgenden Datenschutzrichtlinien bearbeiten kann und dass Sie die Nutzungsbedingungen von EA befolgen.

FALLS SIE DIESEN RICHTLINIEN NICHT ZUSTIMMEN, NUTZEN SIE BITTE KEINE EA-SITE, KEIN(EN) ONLINE- ODER MOBIL-PRODUKT ODER -DIENST. Sollten wir unsere Datenschutzrichtlinien ändern, werden wir diese Änderungen in dieser Datenschutzerklärung, auf den Homepage oder an anderen Stellen veröffentlichen, um Sie darüber in Kenntnis zu setzen, welche Daten wir erfassen, auf welche Weise wir diese nutzen und unter welchen Umständen wir diese, falls zutreffend, weiterleiten. Wir behalten uns das Recht vor, diese Datenschutzerklärung jederzeit zu verändern, schauen Sie deshalb bitte regelmäßig nach. Sollten wir grundlegende oder wesentliche Veränderungen dieser Richtlinien oder bei der Nutzung der Informationen Ihres Kindes vornehmen, werden wir Sie oder die Eltern/Erziehungsberechtigten per E-Mail oder durch eine Benachrichtigung auf unserer Homepage davon in Kenntnis setzen. Ihre weitere Nutzung unserer Online- und Mobil- Produkte und -Dienste stellt Ihre Anerkennung der Veränderungen unserer Datenschutzrichtlinien dar.

INHALT

I. EA Online Datenschutzrichtlinien: Einleitung
II. Die EA Site ist TRUSTe zertifiziert
III. Was sind personenbezogene Daten und wann werden diese von EA erfasst?
IV. Was sind nicht-personenbezogene Daten und wann werden diese von EA erfasst?
V. EA durch Dritte zur Verfügung gestellte Daten.
VI. Was geschieht mit den von EA erhobenen Daten?
VII Wo werden die Daten gespeichert?
VIII Was unternimmt EA zum Schutz Ihrer personenbezogenen Daten?
IX. Überprüfung und Berichtigung Ihrer Daten, Entfernung aus Adressenlisten und Deaktivierung Ihres Kontos
X. Ein besonderer Hinweis zu Kindern
XI. Öffentliche Informationen, einschließlich benutzergenerierte Inhalte, Online-Foren, Blogs und Profile
XII. Webseiten Dritter.
XIII. Produkte, die in Zusammenarbeit mit Dritten angeboten werden
XIV. Kontaktdaten
XV. Einwohner Kaliforniens: Ihre kalifornischen Datenschutzrechte

I. EA Online Datenschutzrichtlinien: Einleitung

EA und seine Tochtergesellschaften respektieren die Datenschutzrechte von Kunden und erkennen die Bedeutung des Schutzes der über Sie gesammelten Informationen an. Wir haben diese globalen Online-Datenschutzrichtlinien eingeführt um zu erläutern, wie wir personenbezogene und nicht-personenbezogene Daten, die wir auf unseren Websites, während Ihrer Nutzung unserer Online-Produkte und oder -Dienste (einschließlich der Online-Spiele) und auf mobilen Plattformen online erfassen, speichern und nutzen. Diese Richtlinien gelten nicht für Daten, die im Rahmen von Stellenausschreibungen online zur Verfügung gestellt werden. Für weitere Informationen lesen Sie bitte die EA-Datenschutzerklärung für Stellenangebote auf der Job-Website von EA unter www.jobs.ea.com.

Diese Richtlinien gelten ebenfalls für TRUSTe-zertifizierte EA Websites. Eine Auflistung dieser geprüften EA-Websites finden Sie unter www.TRUSTe.com. EA besitzt darüber hinaus mehrere andere Domänennamen, die auf die oben angeführten Websites verweisen. Wir können auch neue Sites hinzufügen, die diesen Datenschutzrichtlinien unterliegen, und die Auflistung wird dann aktualisiert, um diese Sites einzubeziehen. Bitte beachten Sie, dass diese Richtlinien nur für Sites gelten, die von EA betrieben werden, und nicht für verlinkte Websites anderer Unternehmen und Organisationen.

EA befolgt das Safe Harbor-Abkommen der Europäischen Union, das vom US-amerikanischen Handelsministerium in Bezug auf die Erhebung, Nutzung und Speicherung von Daten aus der Europäischen Union übernommen wurde und das mit der Datenschutzrichtlinie der Europäischen Kommission von Oktober 1998 übereinstimmt. Informationen in Bezug auf das EU- Safe Harbor-Abkommen finden Sie unter. http://export.gov/safeharbor.

II. Die EA-Site ist TRUSTe-zertifiziert

EA wurde das TRUSTe Datenschutzsiegel verliehen; das bedeutet, dass diese Datenschutzrichtlinien durch TRUSTe auf ihre Übereinstimmung mit den Programmanforderungen von TRUSTe unter http://www.truste.com/privacy_seals_and_services/consumer_privacy/privacy programs requirements.html einschließlich Transparenz, Verantwortlichkeit und Wahlmöglichkeit in Bezug auf die Erfassung und Nutzung Ihrer personenbezogenen Daten geprüft wurden. Die Mission von TRUSTe als unabhängiger Dritter besteht darin, in Bezug auf den Online Verkehr das Vertrauen bei Kunden und Unternehmen weltweit durch seine führendes Datenschutz Trustmark und seine innovativen Loungen zur Vertrauensbildung zu befördern.

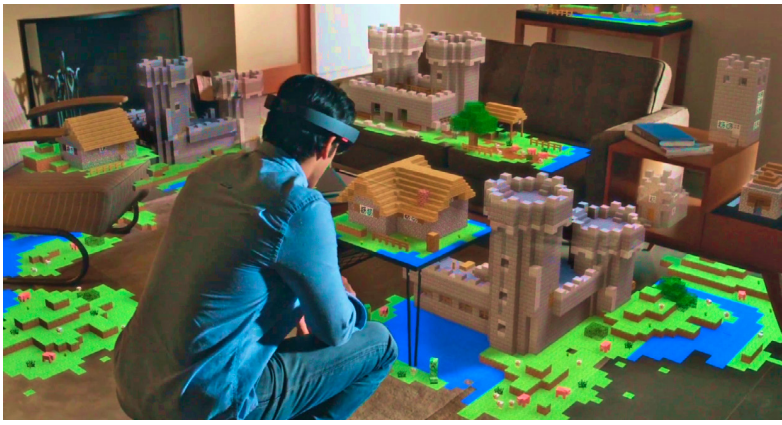
III. Was sind personenbezogene Daten und wann werden diese von EA erfasst?

Kurz vor der Veröffentlichung von Battlefield 3 (links) modelte Electronic Arts seinen Download-Manager zur Vertriebsplattform Origin um. In deren Datenschutzrichtlinien (oben) verbargen sich jedoch diverse rechtliche Fußangeln, EA musste nachbessern.

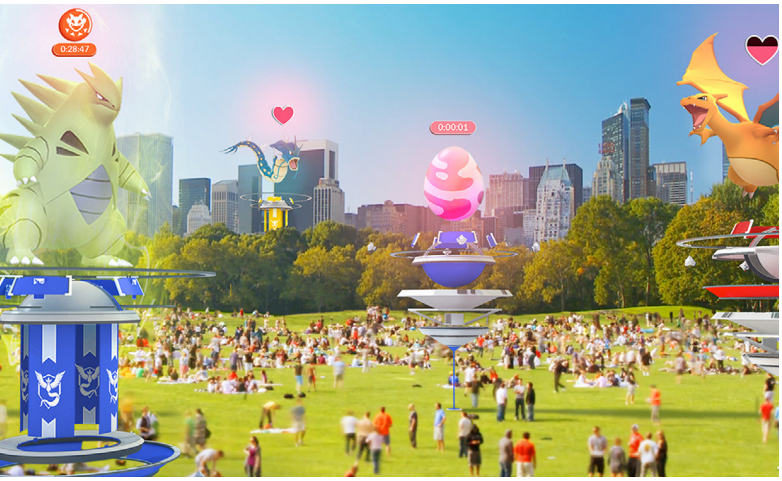
Vereinte EU

Wie also weitermachen in der Datenschutzfrage, zumal sich selbst die deutsche Regierung hinter die Sammelinteressen der datenverarbeitenden Industrie stellt? Angela Merkel etwa mahnte 2015 auf dem IT-Gipfel der Bundesregierung, zu viel Datenschutz schränke den wirtschaftlichen Wettbewerb

Edward Snowdens NSA-Enthüllungen brachten ans Licht, dass die Chats in Second Life teilweise überwacht wurden.



Mit VR- und AR-Hardware wird das Thema Datenschutz auch in Zukunft aktuell bleiben. Firmen wie Facebook oder Microsoft erhalten dank High-Tech-Brillen wie HoloLens (Bild) eine Menge neue und obendrein sehr private Informationen ihrer Nutzer.



Der Hype um Pokémon Go beunruhigte im Sommer 2016 viele Datenschützer. Denn der Entwickler Niantic sammelte GPS-Daten der Spieler und räumte sich das Recht ein, diese auch zu verwenden. Mittlerweile wurden die Datenschutzbestimmungen in Teilen angepasst.

Oculus – hier mit dem kabellosen Headset Oculus Go – sammelt Nutzerdaten nicht nur für sich selbst. Auch der Mutterkonzern Facebook und seine Tochterunternehmen wie Instagram erhalten Zugriff. Nach EU-Recht ist das allerdings verboten.

ein. Stehen Datenschützer auf verlorenem Posten? Im Gegenteil, denn die Europäische Union hat eine neue Datenschutzgrundverordnung auf den Weg gebracht, die einige der Schwachstellen und Ungereimtheiten der bisherigen Regelungen ausräumen soll und auf den wenig klangvollen Namen DSGVO hört. Diese Verordnung gilt für alle Länder der Europäischen Union ab Mai 2018 und vereinheitlich die europäische Gesetzgebung. Zu den wichtigsten Punkten der neuen Verordnung gehört das Prinzip der Zweckbindung, wie es schon im Privacy-Shield-Abkommen festgelegt wurde. Daten dürfen damit nur für den Zweck verwendet werden, für den sie auch erhoben wurden oder für den eine Einwilligung vorliegt. Sobald der Zweck nicht mehr erfüllt ist, müssen die Daten gelöscht werden.

Ein weiteres Prinzip, das ab Mai 2018 gilt, ist »Privacy by Design«, es ist besonders für Videospielfirmen wichtig: »Wer ab dem nächsten Jahr Software programmiert, muss schon bei der Entwicklung darauf achten, dass möglichst wenige Daten erhoben werden, und dokumentieren, wie er sich darüber Gedanken gemacht hat und wie die Daten möglichst sicher verarbeitet werden«, erklärt Kai Bodensiek. »Das heißt, ich muss als Software-Entwickler den Datenschutz von Anfang an im Kopf haben.«
Auch die Meldepflichten wurden verschärft. Sony beispielsweise müsste bei einem erneuten Account-Klau die Nutzer wesentlich früher über den Diebstahl informieren und nicht erst nach einigen Wochen. Unternehmen außerhalb der EU sind ebenfalls dazu verpflichtet, einen hiesigen Ansprechpartner und eine Niederlassung zu nennen, wenn sie Daten von EU-Bürgern verarbeiten. Das soll es erleichtern, die amerikanischen oder asiatischen Unternehmen auf europäisches Recht festzunageln. So wird auch die bisherige Standort-Problematik etwas entschärft, wie es die Rechtsanwältin Ramak Molavi von der Berliner Kanzlei iRights Law erläutert: »Wer im EU-Raum einen Markt hat oder eröffnet, also Dienste für europäische Verbraucher anbietet, der muss sich an die Regeln der DSGVO halten. Wo er seinen eigentlichen Sitz hat, ist unerheblich.« Abkommen wie Privacy Shield werden zwar noch nicht ersetzt, doch schafft die neue Gesetzgebung immerhin mehr Klarheit – auch wenn eine echte Überprüfung schwerfällt, ob die Daten dann schlussendlich in den USA tatsächlich mit der nötigen Sorgfalt verarbeitet werden.

Es wird teuer

Sollten sich Unternehmen nicht an die neuen EU-Vorgaben halten, droht auch ein dickeres Minus für die Jahresbilanz. Statt der bisherigen 300.000 Euro wird das maximale Bußgeld auf 20 Millionen oder vier Prozent des Jahresumsatzes (je nachdem, welche Summe am Ende höher ist) hochgeschraubt. Laut Rechtsanwalt Bodensiek haben die aufgestockten Strafen bereits einige seiner US-Kunden aufgeschreckt, sie würden nun ihre Datenschutzpraktiken überprüfen. »Die werden sich ganz schön umgucken müssen, gerade im Bereich MMO, Browser und Mobile. Da wird sich einiges ändern, was den Datenschutz angeht.« Insgesamt hält er das Gesetz für strenger und umfangreicher: »Man muss den Verbrauchern viel deutlicher erklären, was man mit den Daten macht. Jetzt haben wir einen dreiseitigen Katalog von Dingen, die wir ihnen mitteilen müssen.«

Für den Juristen und Datenschutzrechtler Henry Krasemann muss sich das neue Gesetz aber erst noch beweisen: »Man muss erst mal abwarten. Wir haben alle noch keine Erfahrung in

Unternehmen müssen einen Datenschutzbeauftragten bestellen, sobald dort mehr als neun Personen Zugriff auf die Daten haben.

Datenschutzrichtlinien (hier die von Blizzards Battle.net) sind oft lang, verklausuliert und schwammig. Blizzard gibt hier zudem an, sich an das Safe-Harbor-Abkommen zu halten, das jedoch schon vor zwei Jahren gekündigt und durch ein neues Übereinkommen zwischen den USA und Europa ersetzt wurde. Die Blizzard-Richtlinien wurden zuletzt 2010 aktualisiert.

der Praxis mit dem neuen Gesetz. Auch in dieser Datenschutz-Grundverordnung gibt es wieder Allgemeinplätze beziehungsweise Generalklauseln, die erst mal ausgefüllt werden müssen mit Aussagen der Aufsichtsbehörden und der Rechtsprechung. Es ist noch schwierig zu erkennen, wo genau die Lücken sein werden und wo es in der Praxis Schwierigkeiten geben wird.« Rechtsanwältin Ramak Molavi sieht diese Lücken zum einen im Umgang mit großen Datenmengen: »Das neue Gesetz hat es versäumt, die Frage zu lösen, wie mit Big Data umzugehen ist, zum Beispiel den umfangreichen Datenerhebungen und -verwertungen durch das ›Internet der Dinge‹ oder KI-Systeme. Privacy by Design ist ein wichtiger Schritt, jedoch muss die Regulierung von Innovationen insgesamt wirkungsvoller und vor allem schneller umgesetzt werden, und die Weichen müssen in kürzeren Abständen für die Neuerungen gestellt werden.« Aufgrund des bereits hohen Datenschutzniveaus werden die Anpassungen der DSGVO insgesamt in Deutschland weniger harsch ausfallen. »Endlich kann man sich mit anderen EU-Ländern über Datenschutz auf Augenhöhe unterhalten und gilt nicht als der Exot, wenn man auf Datenschutz Wert legt«, sagt Molavi. Die hohen deutschen Standards gelten so nun auch im Rest der EU.

Datenschutz als Wettbewerbsvorteil

In den mehrjährigen Verhandlungen vom ersten bis zum finalen Entwurf meldeten sich natürlich auch viele Unternehmen im EU-Parlament, die mit personenbezogenen Daten arbeiten und direkt vom Gesetz betroffen sind. Allerdings stellen sie sich nicht, wie man zunächst vermuten würde, einheitlich gegen strikte Datenschutzvorgaben. Viele Unternehmen sehen in der neuen Regelung einen echten Wettbewerbsvorteil gegenüber Firmen, die nur einen laschen Datenschutz besitzen und ihre Kunden im Dunkeln lassen. So erklärt es der Politiker Jan Philipp Albrecht von der Partei Die Grünen. Er war Verhandlungsführer für die DSGVO im europäischen Parlament und spielte damit eine zentrale Rolle bei der Ausgestaltung des Gesetzes. Albrecht spricht

Online-Spiele wie World of Warcraft häufen einen gewaltigen Datenschatz an. Diese Informationen werden oft auf Servern im Ausland gespeichert – was dort damit geschieht, können EU-Behörden bislang kaum kontrollieren.

1. Für Grünen-Politiker Jan Philipp Albrecht haben Unternehmen, die sich an die neue EU-Datenschutzverordnung halten, einen Wettbewerbsvorteil gegenüber Firmen mit laschen Datenschutzbestimmungen. (Bild: Fritz Schumann)

2. Bei der Berliner Kanzlei Brehm & v.Moers berät der Rechtsanwalt Kai Bodensieck deutsche und internationale Spieleunternehmen, auch zum Thema Datenschutz.

3. Der Jurist Henry Krasemann von Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein kritisiert die schwammigen Datenschutzrichtlinien vieler Spielehersteller.

4. Ramak Molavi ist Rechtsanwältin bei iRights Law, einer auf digitale Rechte spezialisierten Kanzlei in Berlin. Sie gehört außerdem zum Managementteam des Berliner Spieleentwicklers Gameduell.

im Zusammenhang mit der DSGVO von einem »vertrauensbildenden Standard«, über den viele Unternehmen glücklich sind, da sich nun alle daran halten müssen. Auch Firmen aus der Videospielbranche zeigen sich offen für bessere Schutzmaßnahmen: »Es haben sich auch viele Spielehersteller gemeldet und sich mit uns getroffen«, erzählt Albrecht. »Sie haben bei mir den Eindruck hinterlassen, dass sie ein großes Interesse daran haben, dass die Nutzerinnen und Nutzer wissen: Hier werden meine Daten nicht verkauft oder zu irgendwelchen Werbezwecken ausgewertet. Jedenfalls nicht, bis ich explizit danach gefragt werde.« Insgesamt sei das neue Gesetz ein wichtiger Schritt in die richtige Richtung, sagt der Grünen- und EU-Politiker: »Ich bin sehr zufrieden mit der Verordnung. Ich glaube, es wird sehr viel dazu beitragen, dass auf dem europäischen Markt aber auch international ein vertrauensvoller Datenschutzstandard als Wettbewerbsvorteil gesehen wird.« Statt sich als Datenkraken jede verfügbare Information zu schnappen, bevorzugen die Spielehersteller also das Vertrauen ihrer Nutzer.

Bezüglich den trockenen, ausufernden und oft im Konjunktiv formulierten Datenschutzerklärungen sieht allerdings auch Jan Philipp Albrecht noch Luft nach oben. Er erwähnt, dass schon seit längerer Zeit überlegt werde, analog zum Jugendschutz auch Datenschutzsymbole einzuführen. Diese würden etwa auf Packungen zu sehen sein und verständlich näherbringen, was mit Nutzerdaten passiere. »Es muss klarer sein, worum es eigentlich geht, wenn man eine Einwilligung zur Datenverarbeitung erteilt.« Die DSGVO hätte dafür den Grundstein gelegt.

Klagen im Namen der Spieler

Auch Nils Büschke vom Verbraucherschutzverband Digitalcourage fordert, dass der Umgang mit (Spieler-)Daten »von Anfang an klar kommuniziert wird und nicht auf einer verklausulierten, juristischen Ebene«. Schließlich hat nicht jeder Spieler ein Jura-Diplom und die Geduld, sich in schwammige Formulierungen einzulesen. Der Verband Digitalcourage vergibt zudem einmal pro Jahr die »Big Brother Awards« für fragwürdige Datenschutzmaßnamen. 2012 ging der »Preis« an Blizzard, unter anderem für verdächtige Softwareüberwachung in WoW und den Real-ID-Skandal. Damals wollten die Kalifornier von allen Forennutzern verlangen, ihren echten Namen preiszugeben.

Wer sich als Verbraucher dagegen beschweren will, kann sich an Verbraucherschutzverbände und auch die Landesdatenschutzbeauftragen eines jeden Bundeslandes wenden. Sie kön-

Nach den neuen EU-Regelungen dürfen die erhobenen Daten nur zum ursprünglichen Zweck genutzt werden – etwa zum Betrieb eines Multiplayer-Spiels wie Fortnite. Wer sie unerlaubt weitergibt, begeht Rechtsbruch.

2011 erbeuteten Hacker persönliche Daten von allen 77 Millionen Nutzern des PlayStation Network. Sony räumte das erst nach einer Woche ein – nach der kommenden EU-Gesetzgebung müsste der PlayStation-Hersteller schneller reagieren.

nen in Datenschutzfragen beraten und teilweise im Auftrag der Verbraucher klagen. Anfang des Jahres 2017 wurde dieses Klagerecht zudem erweitert. Nicht nur staatliche Verbände wie die Verbraucherzentrale Bundesverband können damit juristisch aktiv werden, auch private Vereine wie Digitalcourage: »Entsprechende Verbände und Vereine aus dem Bereich des digitalen Datenschutzes können beantragen, das Verbandsklagerecht nutzen zu dürfen. Dann können Spieler und Spielerinnen Beschwerden an uns richten, woraufhin der Verband eine Musterklage auf den Weg bringen kann.« Wunder solle jedoch niemand erwarten, denn »finanziell sind die Aufsichtsbehörden und Landesdatenschutzbeauftragten in Deutschland und Europa schlecht aufgestellt. Die kommen kaum hinterher«, sagt Büschke. Zum Vergleich: In Bayern arbeiten rund 700.000 Unternehmen mit personenbezogenen Daten in irgendeiner Art und Weise. Ihnen gegenüber stehen 20 Mitarbeiter der Datenschutzbehörde des Freistaates.

Trotz dieser Unterbesetzung hat beispielsweise der Bundesverband Verbraucherschutz schon mehrere Klagen und Unterlassungsverfahren gegen Videospielentwickler und Publisher auf den Weg gebracht. 2012 halfen sie dabei, Electronic Arts zur Lockerung ihrer Origin-Datenschutzbedingungen zu bewegen. Die sehr unkonkret kommunizierte und problematische Datensammlung der mobilen Taschenmonsterjagd Pokémon Go war ebenfalls schon Ziel des Verbandes. So behielt sich deren Entwickler Niantic vor, personenbezogene Daten an Dritte weiterzugeben, was nicht nur Google-Benutzerkonten oder E-Mail-Adressen umfasst hätte, sondern aufgrund der GPS-Ortung sogar regelrechte Bewegungsprofile. Nach einer Abmahnung lenkte Niantic ein und änderte die AGBs. Die Zahl der Verfahren gegen die datenverarbeitende Videospielbranche ist allerdings noch übersichtlich. Weil die Verbraucherverbände die Spiele noch nicht im Fokus haben und sich umgekehrt kaum Spieler bei ihnen melden und Probleme ansprechen. »Videospieler waren bei uns noch nicht«, stellt Nils Büschke fest.

Mit asiatischen Ländern hat die EU kein allgemeines Datenschutzabkommen, mit Firmen wie Nintendo müssen die Behörden oft einzeln verhandeln.

Noch viel zu tun

Bei aller Euphorie über das neue EU-Gesetz finden sich darin auch noch viele strittige Fragen, die erst die Rechtsprechung in der Praxis lösen wird. So bleiben die Standorte der Firmen ein mögliches Schlupfloch. Viele große MMO- und Konsolenanbieter befinden sich auf einem anderen Kontinent, wo auch ihre Hauptserver stehen. Das heißt, dass ein Großteil der Daten weiterhin der direkten Kontrolle der EU-Behörden entzogen ist. Verbraucherschutzverbände wie Digitalcourage kritisieren an der DSGVO zudem, dass sie Unternehmen gestattet, Lösch- und Informationspflichten zu umgehen, wenn ein »unverhältnismäßiger Aufwand« entstehe. So sei zu befürchten, dass Unternehmen ihre Daten zukünftig einfach so speichern, dass jeder Zugriff darauf immer unverhältnismäßig schwierig ist.

Das Aufkommen der Virtual und Augmented Reality öffnet eine weiteres Problemfeld. Unternehmen bekommen hier nämlich nicht nur klassische personenbezogene Informationen wie die Namen und Adressen der Nutzer, sondern auch Daten über deren Wohnfläche und ihre tatsächlichen Sehgewohnheiten. Schließlich könnten die Headsets registrieren, wo der Spieler wie lange hinschaut. Vor allem bei Erotikvideos oder -spielen wäre das rechtlich bedenklich, weil Informationen über die Sexualität unter besonderem Schutz stehen. Laut der Datenschutzbestimmungen sammelt die Oculus Rift bei der Nutzung zudem Informationen über Körperbewegungen und Körpermaße. Ob diese Daten weitergegeben werden, ist unklar, die Datenschutzbestimmungen der Oculus Rift lassen jedoch Böses erahnen. So erhält der Mutterkonzern Facebook alle Daten der Rift, wie auch andere Unternehmen der Facebook-Familie. Und das, obwohl Unternehmen in der EU nicht einfach Datensätze austauschen und kombinieren dürfen, selbst wenn sie zum gleichen Konzern gehören.

Dennoch bleibt die DSGVO ein Schritt in die richtige Richtung, auch für Spieler. Die EU tritt geschlossener auf und spricht mit einer (wirtschaftlich) gewichtigen Stimme. Doch auch einzelne Spieler können aktiver werden und den Umgang mit persönlichen Daten stärker hinterfragen. Sie können Verbraucherschutzverbände konsultieren oder Spielehersteller kontaktieren. Letztere sind verpflichtet, Auskunft darüber zu erteilen, was sie mit den Daten alles anstellen. Es wäre schon ein Anfang, die Datenschutzbedingungen zu lesen – aber wer will das schon? ★