DBSC Infoletter Datenschutz-Praxis 2011-10

Zulässigkeit von Ausweis-Kopien

Im Zusammenhang mit der Zulässigkeit der Vervielfältigung von Personalausweisen und Reisepässen hat das das Bundesministeriums des Innern am 29. März 2011 eine Information bekannt gegeben: Bisher wurde grundsätzlich die Auffassung vertreten, dass das Vervielfältigen von Pässen und Personalausweisen unzulässig sei. Da eine ausdrückliche gesetzliche Regelung fehlt, wird nunmehr die Anfertigung von Ausweiskopien im Einzelfall zugelassen. Insbesondere sei die Erstellung einer Kopie dann zulässig, wenn sie erforderlich ist. Die Kopie von Ausweisdokumenten darf ausschließlich nur zu Identifizierungszwecken verwendet werden und muss als Kopie erkennbar sein. Daten der Betroffenen, die nicht zur Aufgabenerledigung benötigt werden, sind von den Betroffenen zu schwärzen. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen. Die Kopien von Ausweisdokumenten sind unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist. Letztendlich ist eine automatisierte Speicherung der Ausweisdaten nach dem Paßgesetz und Personalausweisgesetz unzulässig.

Feststellung: Es reicht grundsätzlich aus, dass beispielsweise zur Legitimierung der Personalausweis oder der Reisepass vorgelegt und in einem Vermerk schriftlich auf die vorgelegten Ausweisdokumente hingewiesen wird (Handzeichen Sachbearbeiter).

Quelle: Tätigkeitsbericht des LfD Sachsen-Anhalt vom 14.9.2011.

Ergänzender Hinweis des Editors: Personalausweisgesetz PAuswG § 1 Abs. 1 Satz 1, gültig ab 1.11.2010: „Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben."

Online-Spiele – Die Fundgrube zum Datensammeln

Selbst bei Offline-Spielen, die in jedem Kaufhaus oder Elektrogeschäft angeboten werden, ist häufig die Registrierung beim Herstellungsunternehmen notwendig, um das gekaufte Spiel starten zu können. Im Rahmen der Registrierung sollen dann Daten wie beispielsweise Name, Anschrift, Alter, E-Mail-Adresse und Telefonnummer erhoben werden.

Auch wenn bei der nun folgenden Datenerhebung auf den Zweck der Erhebung hingewiesen oder gar eine Einwilligungserklärung zur Datenerhebung und Nutzung eingefordert wird, ist es für die Käuferin oder der Käufer zu diesem Zeitpunkt oft zu spät. Das Geld für die Anschaffung des Offline-Spiels ist bereits entrichtet. Käuferinnen und Käufer sollten schon vor dem Kauf darauf hingewiesen werden, dass das Spielen nur unter bestimmten Voraussetzungen möglich ist.

Bei Online-Spielen geht die Datenerhebung dann noch um ein Vielfaches weiter. Hier werden häufig neben den Registrierungsdaten auch noch ein Pseudonym und ein Passwort erstellt, um den Zugang zum Spiel zu gewährleisten. Bei kostenpflichtigen Spielen kommen Bankverbindungsdaten hinzu. Problematisch ist, dass manche Angebote auch noch weit über das eigentliche Spielen hinaus gehen. Ähnlich wie bei sozialen Netzwerken werden Zusatzdienste wie Freundeslisten, Adressbücher, Nachrichtenübermittlung oder die Erstellung eines weitreichenden Profils angeboten, worin Angaben wie Größe, Augenfarbe, Hobbys und Ähnliches gemacht werden können. Nicht zu vergessen sind solche Daten, die der Internetbrowser der Nutzerinnen und Nutzer standardmäßig übermittelt. Hierzu gehören beispielsweise die IP-Adresse, das genutzte Betriebssystem, der Browsertyp, Datum und Uhrzeit sowie die zuvor besuchte Internetadresse. Schon mit diesen Daten und Informationen können sehr gut Profile erstellt und für Werbezwecke genutzt werden.

Um zu gewinnen, setzen Spielerinnen und Spieler auch unfaire Mittel ein. Mit Hilfe sogenannter Cheat-Programme können Spielsituationen künstlich geschaffen oder sogar Spielstände manipuliert werden. Diese Tatsache wiederum hat Unternehmen motiviert, eine Software zu entwickeln, mittels derer solche betrügerischen Einsatzmittel aufgedeckt werden können. Die Folge dabei ist, dass die ehrlichen Spielerinnen und Spieler einer Spionage auf ihrem Rechner zustimmen müssen, um zu den jeweiligen Spielen zugelassen zu werden. Diese Tools, die eigentlich einen Betrug im Spiel verhindern sollen, können Systemprozesse auslesen und Informationen hieraus an das Unternehmen übertragen, das die Plattform betreibt. Dies geschieht häufig,

ohne dass die Spielerinnen und Spieler sich dessen bewusst sind. Formgerechte Einwilligungen, wie sie das Gesetz vorschreibt, liegen in der Regel nicht vor. Vielmehr beschränken sich die Unternehmen darauf, lediglich diesbezügliche Hinweise in den Teilnahme- bzw. Nutzungsbedingungen oder in den Allgemeinen Geschäftsbedingungen zu geben. Dies ersetzt jedoch nicht eine erforderliche Einwilligung. Problematisch ist zudem, dass auf den Datenschutz gerichtete Regelungen häufig geändert werden und somit für die Spielerinnen und Spieler überraschend sind oder dass diese aufgrund ihres Alters nicht die erforderliche Einsichtsfähigkeit besitzen, um die Gefahren beurteilen zu können.

Feststellung: Die Regelungen und Bedingungen mancher großer Spieleplattformen sind für Benutzerinnen und Benutzer völlig unübersichtlich. Erschwerend kommt hinzu, dass sie in Teilen in fremder Sprache verfasst werden, so dass selbst durchschnittliche volljährige Nutzerinnen und Nutzer kaum in der Lage ist, die dort beschrieben komplexen Datenverarbeitungsprozesse zu verstehen.

Auch wenn die größten Spieleplattformen im Ausland betrieben werden, konnte festgestellt werden, dass Daten oft ohne Rechtsgrundlage verarbeitet werden, anonyme Nutzung nicht ermöglicht wird und viele Vorgänge für die Spielerinnen und Spieler intransparent sind. Aufgrund der Masse der Angebote droht zudem die Gefahr, selbst den Überblick über die Verwendung und Nutzung der eigenen personenbezogenen Daten zu verlieren. Der LfDI NRW empfiehlt deshalb, sich vor dem Kauf oder vor einer Registrierung umfassend über die datenschutzrechtlichen Regelungen zu informieren. Dies gilt insbesondere, wenn es um die Nutzung von Spielen durch Kinder und Jugendliche geht.

Quelle: 20. Datenschutz- und Informationsfreiheitsbericht 2009/2010 des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Facebook Insights unzulässig - Verstoß gegen das Telemediengesetz

Der durch Facebook für die Einbindung von Social-Plugins und Fanpages angebotene Reichweitenanalysedienst „Facebook Insights“ kann nicht über die von Facebook eingeholte „Einwilligung“ datenschutzrechtlich gerechtfertigt werden. § 15 Abs. 3 TMG sieht jedoch zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien vor, dass Nutzungsprofile bei Verwendung von Pseudonymen erstellt werden dürfen. Dies gilt jedoch nur, sofern der Nutzer dem nicht widerspricht. Außerdem hat der Diensteanbieter den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen. Die erstellten Nutzungsprofile dürfen im Übrigen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Betreiber von Fanpages und Webseitenbetreiber, die Social-Plugins von Facebook auf ihren Seiten einbinden, sind nach § 15 Abs. 3 TMG verpflichtet, bei der Erstellung von Nutzungsprofilen auf pseudonymer Basis die Nutzer hierüber sowie über ihre Möglichkeit zum Widerspruch zu unterrichten. Im Fall eines Widerspruchs muss die Profilerstellung unterlassen werden. Dies setzt voraus, dass technisch die Möglichkeit der Widerspruchserteilung implementiert ist. Für Betreiber von Fanpages ist dies nach derzeitigem Wissensstand nicht möglich. Webseitenbetreiber, die Social-Plugins verwenden, müssen sicherstellen, dass eine Übermittlung von identifizierenden Angaben gegenüber Facebook unterbleibt, sobald Nutzerinnen oder Nutzer der Reichweitenanalyse widersprechen.

Feststellung: Wegen der Missachtung des in § 15 Abs. 3 TMG festgelegten Trennungsgebotes ist das Einbinden von Social-Plugins von Facebook in deutschen Webseiten und das Betreiben von „Facebook Insights“ auf Fanpages innerhalb von Facebook unzulässig. Ein Verstoß gegen das Gebot § 15 Abs. 3 S. 3 TMG stellt zugleich eine Ordnungswidrigkeit nach § 16 Abs. 2 Nr. 5 TMG dar, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann.

Quelle: Unabhängiges Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein, Studie „Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook“ vom 19.8.2011.

Link: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf

§ 15 Abs. 1 TMG: Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere 1. Merkmale zur Identifikation des Nutzers, 2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und 3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.