

März 2011

E-Ticketing & Datenschutz

E-Ticketing liegt im Trend: Immer mehr Verkehrsverbünde stellen derzeit auf das moderne System um. Denn die komfortable Art der Bezahlung zieht neue Kunden an. Zugleich erhalten Verbünde detaillierte Informationen zur Liniennutzung und Streckenwahl, die sie für eine kundenorientierte Verkehrsplanung nutzen können. Doch was müssen sie in puncto Datenschutz beachten? Compass, das Kundenmagazin der PTV, hat bei der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich des Innenministeriums Baden-Württemberg nachgefragt.

PTV-Compass: Was sind die Herausforderungen beim Datenschutz, die Verkehrsbetriebe bei der Einführung von E-Ticketing meistern müssen?

Wilko Helmschmidt, als Referent zuständig für Datenschutzfragen im Verkehrswesen: Die Frage lässt sich im Grunde nicht pauschal beantworten, da sich hinter dem Schlagwort "E-Ticketing" verschiedene Modelle bzw. Ausbaustufen eines elektronischen Fahrscheinvertriebs- und Abrechnungsmanagements verbergen können, die in der Praxis überdies teils auch miteinander kombiniert werden. Je nach Ausgestaltung des E-Ticketing variieren die datenschutzrechtlichen Herausforderungen: Während etwa das anonyme bargeldlose Bezahlen mit einer elektronischen Geldkarte kaum datenschutzrechtliche Fragen aufwirft, ist das vollwertige "intelligente" E-Ticketing, in dessen Rahmen jeder Fahrtabschnitt einer Kundenfahrt inklusive etwaiger Umsteigevorgänge mit oder ohne aktive Mitwirkung des Fahrgastes elektronisch erfasst und in einem Hintergrundsystem automatisch abgerechnet wird, mit erheblichen Gefährdungen des informationellen Selbstbestimmungsrechts der Kunden verbunden.

In der Tendenz ist das E-Ticketing im Vergleich zu herkömmlichen Tarifsystemen darauf angelegt, zu Abrechnungszwecken zusätzliche personenbezogene Daten zu generieren, die sich in ihrer Summe zu einem individuellen Bewegungsprofil des Fahrgastes verdichten können. Werden zudem große Datenmengen in einem zentralen Hintergrundsystemen gespeichert, so birgt dies natürlich die Gefahr, dass sie dort von Unbefugten abgegriffen werden könnten. Die Erfahrung zeigt zudem, dass solche Datenbestände stets Begehrlichkeiten, etwa von Seiten der Werbewirtschaft, wecken. Zusätzliche Gefährdungen können zudem aus der Art der eingesetzten Technik erwachsen. So ist es für den Fahrgast zwar sicherlich besonders komfortabel, wenn er sich am Terminal per RFID-Chipkarte kontaktlos ein- und ausbuchen kann, doch könnte eine solche Chipkarte, vom Betroffenen unbemerkt, mithilfe geeigneter Lesegeräte auch von Dritten ausgelesen werden.

Der Verkehrsbetrieb, der das E-Ticketing einführt, steht in der Pflicht, das Verfahren für den Kunden transparent zu gestalten und dessen spezifischen datenschutzrechtlichen Gefahren entgegenzuwirken, indem er geeignete technische und organisatorische Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechts seiner Kunden implementiert. Dem Fahrgast sollte zudem stets die Option verbleiben, die Beförderungsleistungen des Verkehrsunternehmens anonym in Anspruch zu nehmen, ohne Datenspuren im E-Ticketing-System zu hinterlassen.

Compass: Wie sieht das konkret in der Umsetzung aus?

Wilko Helmschmidt: Die technischen und organisatorischen Vorkehrungen zum Schutz des informationellen Selbstbestimmungsrechts haben sich an der konkreten Ausgestaltung des E-Ticketings zu orientieren und können schon deshalb nicht erschöpfend beschrieben werden.

Praktizierter Datenschutz fängt beispielsweise bereits bei der Erhebung der Personalien der E-Ticketing-Kunden an: Das Verkehrsunternehmen sollte von vornherein nur diejenigen Stammdaten des Fahrgastes erheben und speichern, die zu Abrechnungszwecken wirklich benötigt werden. Hierzu gehören regelmäßig sicherlich Vor- und Nachname des Kunden, ferner dessen Postanschrift und im Falle einer Abbuchungsermächtigung auch Bankverbindungsdaten, hingegen z. B. nicht auch das Geburtsdatum – es sei denn, der Kunden hätte einen Sondertarif gewählt, der an das Lebensalter des Fahrgastes anknüpft (z. B. einen Sondertarif für Kinder). Möchte das Verkehrsunternehmen außer der Anschrift weitere Kontaktdaten erheben (Telefon, E-Mail-Adresse), so ist dem Kunden anheim zu stellen, ob er diese Angaben machen möchte.

Um zu vermeiden, dass in der EDV dem einzelnen Fahrgast Bewegungsprofile zugeordnet werden können, sollten die zu Abrechnungszwecken über die Fahrwege der Kunden erhobenen Daten in pseudonymisierter Form separat gespeichert und nicht mit den Kundenstammdaten zusammengeführt werden. Durch die Vergabe differenzierter, abgestufter Zugriffsberechtigungen ist sicherzustellen, dass die Mitarbeiter des Verkehrsunternehmens Zugriff nur auf diejenigen Daten erhalten, die sie unabdingbar benötigen, um ihre Aufgaben zu erfüllen.

Im Interesse der gebotenen Verfahrenstransparenz sollte den Fahrgästen in angemessenem Umfang die Möglichkeit eingeräumt werden, personenbezogene Daten, die auf einem von ihnen mitzuführenden mobilen Speichermedium (Chipkarte) gespeichert werden, jederzeit selbst auslesen zu können. Werden auf der Chipkarte zu Zwecken des Reklamationsmanagements auch Nutzungsdaten gespeichert (etwa: Angaben zu den zuletzt gebuchten Fahrten), so sollte der Fahrgast diese in eigener Verantwortung löschen können. Wird das E-Ticketing als Online-Verfahren betrieben, so bietet es sich ferner an, ein Kundenportal zu implementieren, über das der Fahrgast die zu seiner Person gespeicherten Daten auch selbst einsehen kann.

Nutzungsdaten sollten regelmäßig gelöscht werden, wenn die Abrechnung mit dem Kunden und im Verkehrsverbund abgeschlossen ist. Sollen sie stattdessen in die Verbundstatistik einfließen, so sind sie zuvor zu anonymisieren oder zumindest zu pseudonymisieren.

Compass: In welcher Form dürfen Daten gespeichert werden; was gilt es zu beachten?

Wilko Helmschmidt: Der Grundsatz der Datensparsamkeit gebietet es, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zum angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Daten für Zwecke der Planung und zur Optimierung des Angebots, für die die Identität des einzelnen Fahrgastes ohne Bedeutung ist, sind deshalb nach Möglichkeit von vornherein anonym zu erheben; anderenfalls sind sie alsbald zu anonymisieren oder im Ausnahmefall zumindest zu pseudonymisieren. Pseudonym zu speichern sind ferner auch Daten, die für besondere Leistungsangebote oder das Reklamationsmanagement vorgehalten werden.

Auf die Bedeutung einer differenzierten Zugangsberechtigungsstruktur ist im Übrigen bereits hingewiesen worden. Es gilt zu verhindern, dass Kundenstammdaten von Unbefugten oder nicht autorisierten Bediensteten des Verkehrsunternehmens mit Nutzungsdaten zusammengeführt werden können, um individuelle Bewegungsprofile einzelner Fahrgäste zu erstellen.

Compass: Inwieweit dürfen die Daten analysiert werden?

Wilko Helmschmidt: Es gilt der Grundsatz der Zweckbindung, d. h. die gespeicherten Kundendaten dürfen grundsätzlich nur für den Erhebungszweck, also für die Abbuchung der für den Kunden erbrachten Beförderungsleistungen, verarbeitet und genutzt werden. Die vom Fahrgast mit öffentlichen Verkehrsmitteln zurückgelegte Route darf mithin zunächst erfasst und ausgewertet werden, soweit dies erforderlich ist, um das angefallene Beförderungsentgelt zu errechnen. Diese Kalkulation wird allerdings regelmäßig anhand pseudonymisierter Datensätze erfolgen können; erst die Abrechnungssummen müssen für buchhalterische Zwecke mit den Kundenstammdaten zusammengeführt werden.

Darüber hinaus darf das Verkehrsunternehmen Fahrgastdaten sicherlich statistisch auswerten, um die Auslastung und Wirtschaftlichkeit seines Angebots zu analysieren und seine Geschäftsprozesse zu optimieren; doch müssen die Daten, die in die Statistik einfließen sollen, zuvor anonymisiert oder, soweit anonymisierte Daten hierfür ausnahmsweise nicht hinreichen, zumindest pseudonymisiert werden.

Unzulässig wäre es jedoch beispielsweise, das Fahrverhalten eines Kunden zu analysieren, um diesem ein individuell auf ihn zugeschnittenes Werbeangebot zu unterbreiten - es sei denn, der Betroffene hätte hierzu seine Einwilligung erteilt.

Compass: Wie wird das kontrolliert?

Wilko Helmschmidt: In erster Linie ist es originäre Aufgabe des betrieblichen Datenschutzbeauftragten des Verkehrsunternehmens zu kontrollieren, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Ferner obliegt es der zuständigen Aufsichtsbehörde – im nicht-öffentlichen Bereich ist dies in Baden-Württemberg gegenwärtig noch das Innenministerium – die verantwortlichen Verkehrsbetriebe zu überwachen. Diese ist dabei nicht darauf beschränkt, Beschwerden und Eingaben von Betroffenen nachzugehen, sondern kann durchaus auch Kontrollbesuche vor Ort vornehmen, die keinen besonderen Anlass voraussetzen. Die Erfahrung zeigt im Übrigen, dass die baden-württembergischen Verkehrsverbünde selbst ein großes Interesse an einer datenschutzkonformen Ausgestaltung ihrer Angebote haben und in Zweifelsfragen das Gespräch mit den datenschutzrechtlichen Aufsichtsbehörden suchen. Ein massenhafter Missbrauch von Fahrgastdaten im Zuge der Einführung von E-Ticketing-Modellen im Lande steht deshalb kaum zu befürchten.

Weitere Informationen finden Sie unter:

- ▶ Hintergrundbericht zum Thema „E-Ticketing“:
http://www.ptv.de/fileadmin/files_ptv.de/download/press/files/HB_E-Ticketing_d.pdf
- ▶ Links zur Webseiten Webseite des Innenministeriums Baden-Württemberg: <http://www.im.baden-wuerttemberg.de/de/Datenschutz/83821.html>