Sehr geehrte Teilnehmer an (((eTicket Deutschland,

der Berliner Fahrgastverband IGEB berichtet in einer Presseerklärung vom 28.12.2015 über ein angebliches Datenleck bei der sog. Fahrcard des Verkehrsverbundes Berlin-Brandenburg (VBB). Ein Datenleck – also ein regelwidriges bzw. unkontrolliertes Abfließen von Daten – gibt es jedoch nicht. Auch haben keine Unbefugten den Zugriff auf Daten erhalten. In den Berliner Medien wurde teilweise der Begriff „Spionage“ verwendet – dies entbehrt jeglicher Grundlage.

Die IGEB hat mit Hilfe einer Smartphone-App sowie eines NFC-fähigen Smartphones den Ringspeicher einer vorliegenden VBB-Chipkarte ausgelesen und versucht, mit den so gewonnenen Daten ein Bewegungsprofil zu rekonstruieren.

Die Funktion des Ringspeichers auf den Chipkarten ist eine Servicefunktion im Sinne des Verbraucherschutzes. Diese Funktion gibt dem Fahrgast eine Übersicht über die letzten zehn Transaktionen, die er mit der Chipkarte getätigt hat. Je nach Ausbaustufe Ihres (((eTicket Deutschland Systems können dies reine Kontrolleinträge sein oder tatsächliche Ticketkäufe und damit ein digitaler Kundenbeleg für Reklamationen. Als Kontrolleinträge sind diese vergleichbar mit dem Stempel der Fahrkartenentwerter bei Papiertickets. Dieses Verfahren ist mit den Datenschutzaufsichtsbehörden abgestimmt und im Sinne der Datensparsamkeit auf zehn Einträge begrenzt.

Um Ihrer Pressestelle für mögliche lokale Anfragen Hintergrundinformationen an die Hand zu geben, haben wir die wichtigsten Fakten zum Thema Datenschutz auf der Chipkarte zusammengefasst.

Sollten Sie darüber hinaus Fragen haben, stehen wir Ihnen gerne jederzeit zu Verfügung.

Mit freundlichen Grüßen

[redacted]

[redacted]

[redacted]

Pressebaustein

Bei dem vom Berliner Fahrgastverbands IGEB angesprochenen Datenleck handelt es sich in Wirklichkeit um ein Logbuch, das dem Fahrgast Auskunft über seine letzten zehn getätigten Aktionen mit seinem (((eTicket gibt. Im Sinne des Verbraucherschutzes hat man sich bei der Entwicklung von (((eTicket Deutschland mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder abgestimmt und diese Servicefunktion eingerichtet. Gespeichert werden Zeit und Art der Aktion – ob es sich zum Beispiel um eine Kontrolle oder einen Fahrkartenkauf handelt – sowie eine ID-Nummer die den Ort codiert. Diese Daten werden aber ausschließlich auf der Chipkarte des Fahrgasts gespeichert. Ein mutwilliges Auslesen eines fremden (((eTickets im „Vorbeigehen" ist auf Grund des benötigten Abstands zum Verbindungsaufbau zwischen dem NFC-Chip im Handy und der Chipkarte sehr unwahrscheinlich.

Hintergrundinformationen für VU/VV

1. Datenschutz bei (((eTicket Deutschland

(((eTicket Deutschland wurde in enger Zusammenarbeit mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, sowie dem Düsseldorfer Kreis* entwickelt und realisiert. Hier wurde ein besonderer Fokus auf Datenschutz, Datensparsamkeit und den Verbraucherschutz gelegt. Vor allem soll der Fahrgast die größtmögliche Datentransparenz haben und nachvollziehen können, was mit seinen Daten passiert.

Der Umgang mit allen Daten, die im direkten Kontext der VDV-Kernapplikation verarbeitet werden, entspricht in allen Belangen dem Datenschutzrecht. Die Systemrealisierungen in den jeweiligen Regionen finden in Abstimmung mit den zuständigen Landesdatenschutzbeauftragten statt.

Der Teilnehmerbrief 2/2014 vom 22.12.2014 beschäftigt sich im Detail mit den datenschutzrechtlichen Grundanforderungen für das elektronische Fahrgeldmanagement in Deutschland und hängt dieser E-Mail ergänzend an.

*__Düsseldorfer Kreis__

dient als Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für die Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich.

2. Was wird auf der Karte gespeichert?

Neben den PIN-geschützten Kundenprofildaten befindet sich ein so genannter Ringspeicher mit zehn Speicherplätzen auf der Chipkarte. Dieser dient als Logbuch. Hier wird bei jeder Transaktion ein Eintrag auf die Karte geschrieben. Ab dem elften Eintrag werden die alten Einträge mit den neuen Folgeeinträgen überschrieben, so dass immer nur die letzten zehn Einträge auf der Karte auszulesen sind.

Diese Einträge sind zum Beispiel Kontrolltransaktionen – also wann wurde das Ticket wo auf Gültigkeit geprüft – oder auch der Erwerb einer Fahrberechtigung durch den Check-In an einem Terminal.

Ein solcher für den Fahrgast einsehbarer Eintrag besteht aus der lokalen Kennung des ausführenden Terminals und dem Zeitpunkt und der Art der Aktion (z.B. Check-In, Kontrolle, Check-Out). Zusätzlich können auch Ort, Linie und Fahrt auf der Karte gespeichert werden, insofern die Daten zur Berechnung des Ticketpreises oder aus statistischen Gründen benötigt werden. Hierüber muss der Fahrgast in den Datenschutzbestimmungen bei Abschluss des Vertrages mit seinem Verkehrsunternehmen oder –verbund informiert werden. Der VDV eTicket Service stellt zu diesem Zweck Muster-Datenschutzbestimmungen für die Teilnehmer an (((eTicket Deutschland zu Verfügung.

3. Warum werden Daten auf der Karte gespeichert?

Immer, wenn mit dem (((eTicket an einem Terminal eine Transaktion (z.B. Check-In, Kontrolle, Ticketkauf) ausgeführt wird, die mit dem Schreiben von Daten auf die Chipkarte des Fahrgastes verbunden ist, erfolgt auch eine Prüfung zur Gültigkeit in den Hintergrundsystemen des jeweiligen Verkehrsunternehmen bzw. –verbundes. Der Fahrgast kann im Nachhinein stets selbst prüfen, was mit seinem (((eTicket gemacht wurde. Im Sinne des Verbraucherschutzes besteht so die größtmögliche Datentransparenz. Diese Servicefunktion könnte bei weiterer Verbreitung von Smartphones mit NFC-Chips beispielsweise in die Apps der jeweiligen Verkehrsunternehmen oder –verbünde integriert werden. Das Auslesen der eigenen Chipkarte über das Smartphone des Fahrgasts wäre eine Art digitaler Beleg und Kontrolle der eigenen letzten Fahrten. Eine Erhöhung der Speicherplätze, auch auf Wunsch des Kunden, ist technisch und datenschutzrechtlich nicht möglich.

4. Wer kann die Daten einsehen?

Die Logbucheinträge dienen dem Fahrgast zur eigenen Kontrolle. Die zehn Logbuch-Einträge sind ausschließlich auf der Chipkarte gespeichert. Das Hintergrundsystem, welches z.B. den Kontrolltransaktionsdatensatz gesendet bekommt, speichert immer nur den letzten Datensatz. Kommt ein neuer Kontrolltransaktionsdatensatz an, wird der vorherige gelöscht. Es gibt keinen zentralen Server, der die von Fahrgästen verursachten Einträge länger speichert.

Mitarbeiter von Verkehrsunternehmen haben nur im Kundenzentrum die Möglichkeit, ebenfalls die letzten zehn Transaktionen einzusehen, wenn der Fahrgast seine Karte zu Verfügung stellt. Dies dient einem legitimen Zweck - in diesem Fall dem Bearbeiten von Reklamationen. Das Erstellen von Bewegungsprofilen ist rechtlich untersagt.

Ein zufälliges Auslesen eines fremden Tickets ist ebenfalls nicht möglich. Die Daten werden via NFC (Near Field Communication*) ausgetauscht. Hierzu müssen Sender und Empfänger nah übereinander gehalten werden. Befindet sich das (((eTicket in einem Portemonnaie und dieses in einer Jacken- oder Hosentasche ist selbst das mutwillige Auslesen eines fremden Tickets im Vorbeigehen in der Regel mehr als unwahrscheinlich. Grundsätzlich gilt, dass das (((eTicket genauso wie eine Bank- oder Kreditkarte vor dem ungehinderten Zugriff Unbefugter zu schützen ist.

* Ausführliche Informationen zu NFC im ÖPV finden Sie unter http://oepnv.eticket-deutschland.de/presse-und-medien/

5. Warum ist sind Kontrolltransaktionen wichtig?

Die Kontrolltransaktionen sind - insbesondere in Systemen von Verkehrsverbund oder –unternehmen, die (((eTicket Deutschland nur für Abo-Kunden nutzen - ein wichtiger Baustein zum Monitoring und als relevanter Bestandteil des Sicherheitsmanagements von (((eTicket Deutschland. Bei jeder Kontrolle wird nicht nur geprüft ob die Fahrberechtigung gültig ist, sondern auch ob der übermittelte Datensatz frei von Manipulationen ist. Daher empfehlen wir von Seiten des VDV eTicket Service dringend, die Kontrolltransaktionen gemäß den Spezifikationen der VDV-Kernapplikation als Grundfunktion beizubehalten.

Wichtig ist in diesem Zusammenhang, dass der Kunde bei Abschluss des (((eTicket-Vertrags über die Speicherung der jeweils letzten 10 Transaktionen auf seiner Chipkarte informiert wird.