Abgeordnetenhaus BERLIN

Drucksache 17 / 12 823
Kleine Anfrage

17. Wahlperiode

Kleine Anfrage

der Abgeordneten Katrin Vogel (CDU)

vom 08. November 2013 (Eingang beim Abgeordnetenhaus am 11. November 2013) und **Antwort**

Datenschutz bei der VBB Card

Im Namen des Senats von Berlin beantworte ich Ihre Kleine Anfrage wie folgt:

Die Kleine Anfrage betrifft Sachverhalte, die der Senat nicht aus eigener Zuständigkeit und Kenntnis beantworten kann. Er ist gleichwohl bemüht, Ihnen eine Antwort auf Ihre Anfrage zukommen zu lassen und hat daher den Verkehrsverbund Berlin-Brandenburg (VBB) um eine Stellungnahme gebeten, die von dort in eigener Verantwortung erstellt und dem Senat übermittelt wurde. Sie wird nachfolgend wiedergegeben:

Frage 1: Die Karten sind beim Einlesen an den Terminals dem Kunden zuzuordnen. Ist sichergestellt, dass die Daten nicht gespeichert werden?

Antwort zu 1: Der VBB stimmt jeden Umsetzungsschritt zur VBB-fahrCard im VBB-Tarifgebiet mit den Datenschutzbeauftragten der Länder ab.

Beim Einlesen der Karten an den Terminals wird die Gültigkeit der Applikation und der darauf abgelegten Fahrtberechtigung geprüft. Zudem wird die Kartennummer gegen eine täglich aktualisierte Sperrliste geprüft, um festzustellen, ob die Karte/Fahrtberechtigung aufgrund von Verstößen gegen die Vertragsbedingungen (z.B. Nichtzahlung des monatlichen Abonnementbetrages) zu sperren ist.

Es werden aktuell keine Daten der Kontroll- oder Sperrtransaktion in den Terminal-Hintergrundsystemen gespeichert oder an Drittsysteme weitergegeben. Lediglich auf der Chipkarte wird ein Logbuch geführt, welches die letzten zehn Transaktionen speichert. Der älteste Eintrag wird jeweils durch den neuesten Transaktionsaktionsdatensatz überschrieben.

Frage 2: Falls diese doch gespeichert werden, ist es auszuschließen, dass diese Daten nicht zur Erstellung von Bewegungsprofilen genutzt werden?

Antwort zu 2: Wenn ab voraussichtlich 2015 alle Transaktionsprozesse (z.B. Ticketkontrolle, -ausgabe, -änderung) pseudonymisiert in Datensätzen in den Terminal-Hintergrundsystemen gespeichert und an das verbundweite Hintergrundsystem des VBB übermittelt werden, wird strengstens – und immer in enger Zusammenarbeit mit Datenschutzbeauftragten der Unternehmen und der Länder – darauf geachtet, dass keine Bewegungsprofile erstellt werden. Rückschlüsse zur/zum Kundin/Kunden werden (analog wie z.B. bei EC- und Kreditkarten) nur bei Reklamationen der/des Kundin/Kunden beim vertragshaltenden Verkehrsunternehmen über die Chipkartennummer hergestellt. In den Kontrollsystemen und im verbundweiten Hintergrundsystem des VBB ist es schon allein aufgrund der vorliegenden Daten nicht möglich, Bewegungsprofile zu erstellen. So haben beide Systeme keinen Zugriff auf persönliche Kundendaten, die nur bei den Kundenvertrag führenden Verkehrsunternehmen vorliegen. Nur in Fällen, in denen die Kundin oder der Kunde ausdrücklich aufgrund einer Reklamation die Prüfung ausgewählter Datensätze wünscht, werden diese dem Kundenvertrag führenden Verkehrsunternehmen zur Verfügung gestellt, damit dieses die Reklamation der/des Kundin/Kunden auf dessen Wunsch bearbeiten kann.

Die Transaktionsnachweise, die im zentralen Hintergrundsystem zusammenlaufen, werden nur zu Prüfzwecken verarbeitet, so dass weitestgehend automatisiert und schnell Inkonsistenzen (z. B. fehlerhafte oder unvollständige Transaktionen) erkannt werden können, um entsprechende Maßnahmen einleiten zu können (z. B. Sperrung der Karte/Applikation). Durch diese Prüfverfahren wird die Sicherheit des Systems gewährleistet. Die Transaktionsdaten werden nach einem definierten Zeitraum (voraussichtlich 60 Tage) aus dem System gelöscht.

Frage 3: Wie will der VBB sicherstellen, dass die VBB-fahrCard mit effektiven Maßnahmen gegen das sog. „Cloning“ ausgestattet wird?

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Antwort zu 3: Um das Klonen von Chipkarten auszuschließen, wurden Maßnahmen zur Verhinderung des Auslesens des Dateninhalts ergriffen. In die Systeme wurde ein spezifischer Zugriffsschutz implementiert. Vor jedem Zugriff wird eine gegenseitige Authentifikation zwischen Chipkarte und Lesegerät auf Basis von Zufallszahlen und im Trägermedium gespeicherten geheimen Schlüsseln durchgeführt. Es werden anwendungs- und berechtigungsspezifische Zugriffsrechte und Schlüssel benutzt.

Des Weiteren wird zur Verhinderung von Duplikaten des Trägermediums eine weltweit eindeutige, unveränderbare Kennung des Chips (UID Unit IDentifier) genutzt. Diese Kennung ist in das Konzept zur Zugriffssicherung integriert. Außerdem werden auch optische Sicherheitsmerkmale (Lasergravur) verwendet.

Frage 4: Warum ist das Verfahren so gestaltet, dass alle beteiligten Unternehmen auf die Daten der VBB-fahrCard zu greifen, jedoch der Besitzer nicht?

Antwort zu 4: Die VBB-fahrCard kann auch von allen Kundinnen und Kunden an selbst zu bedienenden Infoterminals ausgelesen werden, die viele Verkehrsunternehmen im Verbund an zentralen Standorten installieren. Zudem gibt es Apps für NFC-Smartphones, mit denen die Dateninhalte der Karte ausgelesen werden können. In einer späteren Ausbaustufe soll es möglich sein, dass Kundinnen und Kunden ihre Abonnements online von zu Hause mit Hilfe eines entsprechenden Chipkartenlesegeräts verwalten und somit auch Dateninhalte direkt einsehen können.

Frage 5: Wie setzt sich der hohe Verwaltungskostenaufwand (20 €) beim Verlust der Karte zusammen?

Antwort zu 5: Die Kosten für den Kunden bei einmaligem Verlust betragen 10 Euro. Jede weitere Neuausstellung einer VBB-fahrCard binnen 24 Monaten nach Ausstellung der ersten Ersatzkarte kostet 20 Euro.

Es soll vermieden werden, dass Kundinnen und Kunden als verloren gemeldete Karten an andere Personen zur unberechtigten Nutzung weitergeben. Die weitergegebenen Karten könnten bis zu einer ersten elektronischen Kontrolle genutzt werden. Zudem soll vermieden werden, dass Kundinnen und Kunden aufgrund der Möglichkeit des Ersatzes unachtsam mit ihrer VBB-fahrCard umgehen.

Frage 6: Wie wird sichergestellt, dass Kundendaten nicht auf den mobilen Terminals der Kontrolleure missbraucht werden?

Antwort zu 6: Mit den mobilen Kontrollterminals der Kontrolleurinnen und Kontrolleure werden lediglich die Daten zur zeitlichen und räumlichen Gültigkeit, die für die Kontrolle relevant sind, von der Chipkarte ausgelesen und angezeigt. Nur bei persönlichen Abonnements werden (analog zur heutigen Kundenkarte) die persönlichen Daten angezeigt (Kundenname und bei Abonnements, die an ein gewisses Alter gekoppelt sind, das Geburtsdatum). Es werden aktuell jedoch keine kundenbezogenen Datensätze in den Terminals gespeichert. Wenn ab 2015 Transaktionsdatensätze erzeugt und an die Terminal-Hintergrundsysteme weitergegeben werden, wird durch entsprechende Zugriffsprofile sichergestellt, dass Kontrolleure keinen Zugriff auf die Datensätze erhalten.

Frage 7: Wird sichergestellt, dass nur relevante Daten auf der Karte gespeichert werden, die keinen Rückschluss auf das Kundenverhalten zulassen?

Antwort zu 7: Die Datenstrukturen auf dem Chip der VBB-fahrCard sind von der VDV[1]-Kernapplikation GmbH & Co. KG, die den durch Bund und Länder geförderten technischen und organisatorischen Standards für elektronisches Fahrgeldmanagement in Deutschland festlegt, verbindlich vorgeschrieben. Der VBB und alle Verkehrsunternehmen im Verbund sowie zahlreiche weitere Verkehrsunternehmen und -verbünde in ganz Deutschland haben sich zu deren Einhaltung vertraglich verpflichtet. Änderungen an vorhandenen oder Ergänzungen weiterer Datenfelder sind also nur innerhalb der vorgegebenen Datenstrukturen möglich. Somit ist es keinem Verkehrsverbund oder Verkehrsunternehmen erlaubt, nachträglich individuelle Datenfelder einzuführen.

1) Verband Deutscher Verkehrsunternhmen

Frage 8: Wie kann sichergestellt werden, dass der Besitzer einer Karte beim Missbrauch der Daten seiner Karten (Cloning) keine Nachteile in Form von sofortigem Einzug der Karte, Kosten für die neue Karte etc. erfährt?

Antwort zu 8: Ein „Cloning“ der Karte ist nach dem derzeitigen Stand der Technik ausgeschlossen (vgl. Frage 3). Darüber hinaus ist durch das in das Gesamtsystem integrierte Sicherheitsmanagement sichergestellt, dass – sollten jemals gefälschte Chipkarten im System auftauchen – diese im Prüfprozess sofort erkannt werden. Sollte dann eine gefälschte Karte ein zweites Mal im System auffallen, wird die/der rechtmäßige Besitzerin/ Besitzer der Original-VBB-fahrCard umgehend informiert und erhält eine neue Karte. Das Kontrollpersonal würde ebenso sofort über die Sachlage der betroffenen Kartennummer informiert, so dass der Kundin oder dem Kunden keine unnötigen Nachteile entstehen. Es würden der Kundin oder dem Kunden keine Kosten entstehen.

Berlin, den 13. Januar 2014

In Vertretung

C h r i s t i a n G a e b l e r

.....

Senatsverwaltung für Stadtentwicklung und Umwelt

(Eingang beim Abgeordnetenhaus am 23. Jan. 2014)