

675.35.16

Arbeitspapier E-Ticketing in öffentlichen Verkehrsmitteln

– Übersetzung –

Angenommen auf der 42. Sitzung, 4-5. September 2007, Berlin

1. Die technologische Entwicklung im Bereich der Chipkarten und das Streben nach erhöhter Effizienz und Kosteneffektivität beim Management von Dienstleistungen im öffentlichen Verkehr – dies betrifft integrierte Eisenbahnen, U-Bahn und Flächentransportdienstleistungen – haben zu einer wachsenden Nutzung innovativer E-Ticketing Systeme geführt.

Solche Systeme arbeiten mit elektronischen Karten, die gewöhnlich personalisiert sind und die vornehmlich für Transportdienstleistungen, aber zunehmend auch zur Bezahlung damit zusammenhängender anderer Leistungen genutzt werden können (z.B. für elektronische Bezahlung von Parkgebühren bei Pendlern)¹.

2. Die Chipkarten enthalten einen Mikroprozessor, der Informationen einschließlich personenbezogener Daten speichert (dazu können z.B. die Chipidentifizierungsnummer, die Nummer des Abonnements des Benutzers sowie die Zeit, das Datum und die Nummer des Gerätes zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gehören); in manchen Fällen arbeiten sie mit RFID/Near Field Communication (NFC) Technologie.

Die Nutzung solcher Chipkarten beinhaltet daher die Verarbeitung von verschiedenen unmittelbar und/oder mittelbar zuordenbaren personenbezogenen Informationen:

- Zu dem Zeitpunkt, zu dem die Karten an die Benutzer ausgegeben werden;
- Jedes Mal, wenn die Karten benutzt werden, dank der Identifikationsnummern, die jedem Abonnenten zugeordnet sind und die durch Geräte zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gesammelt und dann möglicherweise in Echtzeit in den Datenbanken der Transportunternehmen gespeichert werden.

In diesem Kontext müssen besonders die so genannten Validierungsdaten (Daten über die Entwertung oder Überprüfung der Gültigkeit) beachtet werden, deren Verarbeitung – insbesondere die Speicherung von Zeit und Ort der Entwertung oder Überprüfung – es ermöglicht, die Bewegungen und Aufenthaltsorte einzelner Benutzer zu verfolgen.

¹ Andere Zahlungsformen sind z.B. Barzahlung, Zahlung über Mobiltelefon, etc.

3. Die Informationen, die öffentliche Transportunternehmen im Rahmen der Erbringung ihrer Dienstleistungen verarbeiten, einschließlich der Informationen, die zum Zeitpunkt der Entwertung oder Überprüfung der Karte gespeichert werden, können für verschiedene Zwecke genutzt werden, wie z.B.:

- die Bereitstellung von Transportdienstleistungen,
- die Bekämpfung von Betrug beim E-Ticketing (wenn Chipkarten verloren, gestohlen oder ohne Autorisierung kopiert werden),
- Werbung,
- die Aufteilung der Einnahmen unter verschiedenen Beteiligten, wenn öffentliche Transportdienstleistungen gemeinsam durch mehrere Transportunternehmen erbracht werden,
- die Analyse aggregierter Daten über Verkehrsflüsse, um die Effizienz der erbrachten Dienstleistungen zu steigern.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

Vorabkontrolle (Privacy Impact Assessment)

Das Recht der Kunden auf den Schutz ihrer personenbezogener Daten muss bereits beim Entwurf und im Rahmen der Entwicklung von Informationssystemen der Transportunternehmen berücksichtigt werden; grundsätzlich sollten das Recht auf persönliche Freizügigkeit und die Anforderungen effizienten öffentlichen Verkehrs miteinander in Einklang gebracht werden.

Anonymität

Verkehrsbetriebe und Transportunternehmen sollten ihren Kunden alternativ Möglichkeiten zur anonymen Nutzung (ohne unbillige Hindernisse) anbieten, z.B. Barzahlung oder anonyme E-Tickets.

Wo Anonymität aus technischen Gründen nicht angeboten werden kann, müssen die folgenden Empfehlungen beachtet werden:

Datenschutzinformation und Transparenz

Verkehrs- oder Transportunternehmen, die E-Ticketing-Systeme nutzen, sollten die Betroffenen unmissverständlich über die Verarbeitung ihrer personenbezogenen Daten informieren. Die Betroffenen sollten in der Lage sein, die spezifischen Zwecke leicht zu verstehen, die von den Unternehmen verfolgt werden, welche Arten von personenbezogenen Daten über sie gesammelt und gespeichert werden, und wie diese Informationen genutzt werden.

Datensparsamkeit und Speicherdauer

Insbesondere in Bezug auf die Verarbeitung der Reisedaten der Nutzer sollten die Informationssysteme von Transportunternehmen so geplant und entwickelt werden, dass sie die Nutzung anonymer Daten priorisieren. Wenn (direkt oder indirekt) personenbezogene Daten genutzt werden, sollten diese Informationen für die kürzestmögliche Zeitdauer gespeichert (und danach gelöscht) und die gesetzliche Zweckbestimmung der Verarbeitung beachtet werden – grundsätzlich sollten die betreffenden Informationen nicht länger als ein paar Tage nach ihrer Erhebung gespeichert bleiben.

Sicherheit

Die Sicherheitsmaßnahmen beim Zugriff auf personenbezogene Daten sollten ein Überwachungssystem zur Verhinderung des Missbrauchs von Informationen umfassen. Verkehrsunternehmen sollten sicherstellen, dass der Schutz der Privatsphäre registrierter Nutzer garantiert wird, wenn sie ihren Partnern und ihren eigenen Mitarbeitern den Zugriff auf ihre Datenbanken eröffnen.

Werbung

Ein Verkehrs- oder Transportunternehmen sollte die freiwillige und informierte, vorherige Einwilligung seiner Kunden für die Nutzung personenbezogener Daten für eigene Werbezwecke oder die

Nutzung durch verbundene Partnerunternehmen für unverlangte Werbung gegenüber dem Reisenden einholen. Diese Einwilligung sollte sich von der Zustimmung zu allgemeinen Geschäftsbedingungen unterscheiden.

Zahlungsnachweis

Soweit z. B. zur Kostenerstattung oder aus steuerlichen Gründen ein Zahlungsnachweis über einzelne Reisen erforderlich ist, sollten dafür datenschutzfreundliche Lösungen angeboten werden.

Verhaltensregeln

Die Entwicklung von Verhaltensregeln zum Datenschutz sollte gefördert werden. Insbesondere im Hinblick auf die Verarbeitung von Bewegungsdaten der Nutzer sollten Informationssysteme von Transportunternehmen unter Priorisierung der Nutzung von anonymen Daten geplant und entwickelt werden.

Systemdesign

Die Systementwicklung sollte so erfolgen, dass personenbezogene Daten von Reisedaten getrennt werden (2-Komponenten-Modell). Eine zentrale Speicherung sollte auf aggregierte und/oder anonyme Transaktionen beschränkt werden. Karteninhaber sollten Daten über die Nutzung ihrer Karten kontrollieren können.