eTicket Service

(((eTicket Deutschland

Teilnehmerbrief

Thema: Datenschutz

22. Dezember 2014

Inhaltsverzeichnis

Editorial

Sehr geehrte Teilnehmer an (((eTicket Deutschland,

in der Entwicklung von (((eTicket Deutschland erhielt der Datenschutz von Beginn an einen besonderer Stellenwert. Die Fahrgäste sind bei diesem Thema zunehmend sensibilisiert und wollen wissen, was mit Ihren Daten geschieht. Sie verlassen sich darauf, dass wir sorgsam und vollumfänglich der gesetzlichen Rahmenbedingungen mit personenbezogenen Daten umgehen. Das Bewusstsein, dass Daten die Währung in der digitalisierten Welt sind, ist in der Mitte der Gesellschaft angekommen.

Die datenschutzrechtlichen Grundanforderungen für das elektronische Fahrgeldmanagement in Deutschland wurden mit den Datenschutzbeauftragten des Bundes und der Länder entwickelt und abgestimmt. Die insgesamt elf Anforderungen sind zum einfacheren Verständnis direkt mit ihren Maßnahmen zur Erfüllung tabellarisch im folgenden Dokument gegenübergestellt.

Die Ergebnisse dieses Dokumentes sind in das (((eTicket-Regelwerk und die Feinspezifikationen der VDV-Kernapplikation eingeflossen. Um zu vermeiden, dass Sie mit den für Sie zuständigen Datenschutzbeauftragten Fragen bearbeiten, die bereits beantwortet worden sind, stellen wir Ihnen die abgestimmten Regelungen hiermit vollständig zu Verfügung. Mit dem als Anlage beigefügten Schreiben vom 30. Oktober 2012 der berichterstattenden Datenschutzbeauftragten des Landes NRW wurden die Abstimmungen zum Datenschutz für das elektronische Fahrgeldmanagement in Deutschland für abgeschlossen erklärt.

Für Fragen zu diesem Thema stehen wir Ihnen gerne zu Verfügung.

Mit freundlichen Grüßen

Klaus Hoffmann
Leiter Beschaffung und Vertragswesen

Telefon: 0221/716174-113
Telefax: 0221/716174-213
E-Mail: hoffmann@vdv.de

Gemeinsame Datenschutz-Standards für das elektronische Fahrgeldmanagement

In der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25.10.2002 in Trier wurde ein von dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LfD NRW) vorgelegtes und in einer Arbeitsgruppe abgestimmtes Papier zu „Datenschutzrechtlichen Grundanforderungen“ für das Elektronische Fahrgeldmanagement (EFM) einstimmig zustimmend zur Kenntnis genommen.

Beim Treffen der Arbeitsgruppe Datenschutz des VDV mit Vertretern der Datenschutzbeauftragten und Aufsichtsbehörden am 30. Juni 2008 wurde den Vertretern der Datenschutzbehörden präsentiert, in welcher Weise diesen Grundanforderungen in den Spezifikationen der VDV-Kernapplikation für elektronisches Fahrgeldmanagement als Basisstandard für ein (((eTicket Deutschland Rechnung getragen worden ist bzw. werden soll.

In einem Abstimmungsgespräch am 19. August 2008 beim Berliner Beauftragten für Datenschutz und Informationsfreiheit (Bln BDI), das ursprünglich der datenschutzrechtlichen Begleitung der Erstreckung des EFM auf die europäische Ebene dienen sollte, wurde seitens der Vertreter der VDV eTicket Service GmbH & Co. KG (ehem. VDV-Kernapplikations GmbH & Co. KG) der Wunsch laut, dass gemeinsame Datenschutzstandards für alle Verkehrsunternehmen, die mit der Kernapplikation arbeiten wollen, formuliert werden sollten.

Zunächst werden hier die datenschutzrechtlichen Grundanforderungen den Maßnahmen zu ihrer Erfüllung tabellarisch gegenübergestellt werden.

Tabellarische Übersicht

1. Transparenz Die Datenverarbeitung durch das EFM muss transparent sein (§ 6 c Abs. 1 Nr.2 und 3 BDSG). Dies erfordert die * Festlegung der Zwecke, * Beschreibung der einzelnen Datenverarbeitungsvorgänge differenziert nach den jeweiligen für den Fahrgast zutreffenden Geschäftsprozessen und die dabei zu verarbeitenden Daten, * Angaben der Identitäten und Anschriften der Stellen, die zu den genannten Zwecken personenbezogene Daten verarbeiten und/oder bei denen die jeweiligen Rechtsansprüche geltend gemacht und Verfahrensbeschreibungen gem. § 4g Abs. 2 Satz 2 BDSG eingesehen werden können. * Einbeziehung der Unterrichtungspflichten der Kundenvertragspartner. Dazu sollte ein Merk- oder Informationsblatt erstellt werden, in dem der Fahrgast in allgemein verständlicher Form über die vorgesehene Datenverarbeitung - auch durch zentrale Servicestellen oder andere autorisierte Dritte - und über seine Rechte nach §§ 34,35 BDSG unterrichtet wird.	Es wird ein Informationspapier mit verbindlichen Inhalten (Anlage s. Anlage Datenschutzhinweise) bereitgestellt zur Beschreibung der Datenverarbeitungsvorgänge und der Daten, die im Nutzermedium (Chipkarte) gespeichert werden. Dieses Papier wird durch den Kundenvertragspartner zur Verfügung gestellt. Wesentliche Inhalte des Informationspapiers sind in der sog. Kundenschnittstellenspezifikation enthalten, die Bestandteil der einzuhaltenden KA-Spezifikationen und EFM-Teilnahmeverträge der teilnehmenden Unternehmen ist. Ferner werden die Teilnehmer am EFM (Kundenvertragspartner) den Endkunden im Zusammenhang mit dem „Antrag auf Ausgabe einer eTicket-Karte (Nutzermedium)“ zur Ausstellung des Kundenmediums Datenschutzhinweise übergeben.
2. Widerspruchsrecht Der Verband der Deutschen Verkehrsunternehmen sollte mit seinen Kundenvertragspartnern verabreden, dass der Kunde bei Vertragsabschluss schriftlich erklärt, ob er der Übermittlung oder Nutzung seiner Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung widersprechen möchte oder nicht. Es ist sicherzustellen, dass auch autorisierte Dritte diese Beschränkung beachten.	Im „Vertrag über die Teilnahme am VDV EFM-Standard als Kundenvertragspartner (KVP)“ (Teilnahmevertrag zwischen VDV-eTicket Service GmbH & Co. KG als Applikationsherausgeber für die VDV-Kernapplikation und (Verkehrs-) Unternehmen, die als Kundenvertragspartner im EFM-System auftreten; liegt als Vertragsentwurf vor) ist eine Verpflichtung für Unternehmen aufzunehmen, die die Rolle eines Kundenbetriebspartners einnehmen.

3. Wahlmöglichkeit Den Fahrgästen muss nach Information über die vertraglich bedingte Datenverarbeitung eine freie Entscheidung zwischen anonymer Fahrt und besonderen Leistungsangeboten (bspw. best pricing) überlassen bleiben.	Der Fahrgast kann zwischen anonymen/pseudonymen (auch gegen Barzahlung) und personalisierten elektronischen Tickets (z. B. Jobtickets, Schülertickets) wählen. Die Kernapplikation sieht zum Erwerb von Fahrtberechtigungen bzw. zur in Anspruchnahme von ÖPV-Leistungen vor: * Berechtigungen mit auf dem Nutzermedium gespeicherten Werteinheiten (mit Schattenkonto bei Kundenvertriebspartner) * anonyme Berechtigungen mit Abrechnung nach Vorauszahlung auf ein Kundenkonto und Abbuchung der Leistung gegen vorausbezahlten Betrag * pseudonyme Berechtigung durch Bezahlung mittels Lastschrifteinzugsverfahren (Bankkonto gebundene eTicket-Karte)
4. Datensparsamkeit Alle Leistungsmerkmale und Geschäftsprozesse sind nach dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a Bundesdatenschutzgesetz) zu gestalten. Insbesondere ist auszuschließen, dass kundenbezogene Bewegungsprofile erstellt werden. Das bedeutet: * Daten für Planungszwecke und zur Optimierung des Angebots sind anonym zu erheben oder zu anonymisieren; * soweit Daten für besondere Leistungsangebote oder das Reklamationsmanagement benötigt werden, sind diese pseudonym zu erheben und zu speichern, so dass ohne Wissen und Wollen des betroffenen Fahrgastes eine Zuordnung zu seiner	Das Sammeln von Daten in den Systemen zu Abrechnungs- und Planungszwecken und für die Optimierung von Reiseangeboten geschieht generell ohne Zuordnung zu einer Person – es werden nur Daten verknüpft, die zu diesem Zweck benötigt werden. Bei der ÖPV-Nutzung erfasste Leistungsdaten zur automatisierten Fahrpreisfindung (IN/OUT) werden „alias“ gespeichert und nur bei der Abrechnung einer Person zugewiesen (dem Kontoinhaber). Sie dürfen danach nur für die Dauer der zulässigen Reklamationszeiten durch den Fahrgast gespeichert bleiben und sind nach Ablauf der Frist (sofort zu löschen (vgl. Pkt. 11). Die zulässigen Reklamationszeiten richten sich nach z.B. der Fahrgastrichtlinie.

Person ausgeschlossen ist; * werden zu Zwecken des Reklamationsmanagements nutzungsbezogene Daten auf mobile Speichermedien (Chipkarte) geschrieben, muss es dem Fahrgast ermöglicht werden, diese Daten auf eigene Verantwortung zu löschen. Die Verarbeitung dieser Daten außerhalb dieser durch das Berechtigungsmanagement geschützten Anwendungsprozesse ist nur zulässig sofern dies ohne personenbezogene Daten erfolgt. Insofern darf ein Export dieser Daten nicht möglich sein.	Gebrauchsbezogene Daten in dem Nutzermedium werden beim nächsten Gebrauch überschrieben (max. 10 Transaktionen werden im Medium gespeichert, insbesondere damit der Kunde die letzten Nutzungen auslesen kann, wenn er dies wünscht.) Diese Transaktionen werden auch an das für die genutzte Fahrtberechtigung zuständige Hintergrundsystem weitergeleitet. In KA NM-SPEC spezifizierte Inhalte der Transaktionen sind notwendig als Element des Sicherheitskonzepts. Sie sind festgelegt mit: o Zeitpunkt o Ort ID, Fahrt ID, Linien ID: könnten evtl. gestrichen werden (nicht benutzte Datenelemente mit 0x00 füllen) o Typ des Terminals: kann 0x00 sein (ist Bestandteil der Terminal_ID) o Terminal ID: Muss Element o SAM ID: Muss Element o Produkt ID: Muss Element o Berechtigungs Nr.: Muss Element o Daten der MAC Sicherung: Muss Elemente Alle weiteren Informationen werden nur dann gefüllt (ungleich 0x00), wenn sie im Geschäftsprozess zwingend erforderlich sind.

5. Getrennte Verarbeitung Es müssen die jeweils erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Nr.8 der Anlage zu § 9 BDSG).	Die Kundenvertragspartner werden von der VDV eTicket Service im Teilnahmevertrag verpflichtet, Kundenstammdaten oder Rechnungsdaten in separaten Systemen zu speichern, so dass keine Kunden bezogene Bewegungsprofile erstellt werden können. Die Daten werden nur zum Zweck der Abrechnung zusammengebracht. Das Personal des Kundenvertragspartners, welches die persönlichen Daten verarbeitet, wird zum Datenschutz und zur Einhaltung des Telefongeheimnisses gem. BDSG und LDSG verpflichtet.
6. Zweckbindung der Ticketdaten Darüber hinaus dürfen keine kunden- oder kartenbezogenen Auswertungen zu fremden Zwecken erfolgen. Zu Abrechnungszwecken im Verkehrsverbund dürfen allenfalls (pseudonyme) kartenbezogene Daten übermittelt werden.	Die Spezifikation sieht vor, dass nur kartenbezogene (d. h. „Berechtigungs“ bezogene) Daten zu Abrechnungszwecken zwischen EFM Systembetreibern kommuniziert werden dürfen. Kundenbezogene Daten dürfen nur mit schriftlichem Einverständnis der Kunden und durch seinen eigenen Kundenvertragspartner erstellt werden. Der Kunde wird im „Antrag auf Ausgabe einer eTicket-Karte (Nutzermedium)“ auf die Art der Datenverarbeitung hingewiesen, auch wenn dieser Vertrag im Fall des Erwerbs einer anonymen Berechtigung nicht zwingend ausgefertigt wird.
7. Vorabkontrolle Von dem oder der betrieblichen Datenschutzbeauftragten ist vor Inbetriebnahme des EFM eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG) und zu dokumentieren.	Diese ist durch den EFM-Systembetreiber zu gewährleisten. In den KA-Teilnahmeverträgen für die an der KA teilnehmenden Unternehmen ist auf diese Verpflichtung hinzuweisen.

8. Zugriffsberechtigung Der Lesezugriff für Kontrollpersonal muss auf die zur Kontrolle notwendigen Daten beschränkt sein, insbesondere auf dem Speichermedium des Fahrgastes.	Es werden nur räumlich und zeitlich gültige Berechtigungen kontrolliert. Ist eine Personalisierung der Applikation vorhanden, ist das Kundenprofil kryptographisch gesichert. Der Zugriff auf das Kundenprofil ist nur über eine asymmetrische Authentisierung zwischen Terminal und Nutzermedium möglich oder nach Eingabe einer PIN durch den Kunden. Personalisierte Berechtigungen werden nur in Ausnahmefällen durch Eingabe von Daten in ein Kundenprofil umgesetzt. Meist sind die Personendaten nur im Hintergrundsystem gespeichert. Die Nutzer bezogenen Daten werden nur beim Prozess der Ticket-Kontrolle durch das Kontrollpersonal eingesehen und nicht elektronisch zur weiteren Verarbeitung gesammelt. Persönliche Daten (Name, Vorname, Geschlecht, Geburtsdatum) werden in der Berechtigung gespeichert, wenn diese personenbezogen kontrolliert werden muss (z. B. Schüler, Studenten)
9. Datenschutzgerechte Gestaltung der Systemkomponenten Die Systemkomponenten, die von Fahrgästen bedient werden, sind datenschutzgerecht so zu gestalten, dass * keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten zur Kenntnis zu nehmen, * Fehlermeldungen der Zugangs-Erfassungssysteme die Betroffenen nicht	Automatische Kontrollen und die Datenerfassung durch Terminals werden nur mit anonymen Berechtigungsdaten durchgeführt. Alle Transaktionen werden erst nach einer Authentisierung durchgeführt. Kundendaten an selbst bedienten Verkaufsterminals / im Internet werden erst nach Eingabe einer PIN angezeigt (VDV KA-KUSCH-Spec)

öffentlich diskriminieren, * die Fahrgäste in angemessenem Umfang die Möglichkeit haben, den Inhalt der Chipkarte jederzeit auslesen zu können.	Dienstleistungen per Telefon werden erst nach einer Passwort-Authentisierung durchgeführt. Fehlermeldungen in Verbindung mit dem Vorweisen des Nutzermediums an Geräten mit einer Kundenschnittstelle werden nicht den Grund für den Fehler enthalten.
10. Schutz gegen Missbrauch Es müssen Vorkehrungen (u.a. Sperrung, Verschlüsselung) getroffen werden, die den Fahrgast in angemessener Weise gegen missbräuchliche Verwendung der Daten durch Dritte bei Verlust des Speichermediums schützen.	Die Applikation und einzelne Berechtigungen können durch den Kunden gesperrt werden. Es erfolgt aus Performance-Gründen keine Verschlüsselung beim Zugriff auf das Applikationsverzeichnis und auf Berechtigungen. Berechtigungen werden mit codierten Datenelementen gespeichert und für die Verarbeitung in verschiedenen EFM-Systemen übermittelt. ORG-IDs, die von der VDV eTicket Service vergeben werden sind vertraulich. Nummercodes für Orte/Haltestellen/Bahnhöfe werden nicht veröffentlicht. Schreibvorgänge und Transaktionen werden generell nur nach kryptographischer Authentisierung ausgeführt und mit einer Signatur gesichert.
11. Löschung Die Dauer der für die bestimmten Geschäftsprozesse erfolgenden Speicherung personenbezogener Daten muss so kurz wie möglich sein. Für die jeweiligen Geschäftsprozesse sind Regelfristen für die Löschung der Daten festzulegen (§ 4e Satz 1 Nr. 7 BDSG). In den Terminals gespeicherte Daten sind nach erfolgreicher Datenübertragung an den Rechner des Kundenvertragspartners zu löschen.	Die Löschung von Daten muss von den über einen Teilnahmevertrag verpflichteten EFM-Systembetreibern garantiert werden. Die Zeitlimits werden abhängig von den Geschäftsprozessen definiert und mit dem verantwortlichen DSB koordiniert.

Anforderungen

Aus diesen Anforderungen der Arbeitsgruppe der Datenschutzbehörden und den Ausführungen zu ihrer Umsetzung ergeben sich bereits die Anforderungen, die sich an die sog. Kundenvertragspartner (aber z. T. auch an die EFM-Systembetreiber) richten:

1. Zur Sicherstellung der Transparenz für die Kunden haben die Kundenvertragspartner dem Nutzer ein Informationspapier zur Verfügung zu stellen, in dem die Datenverarbeitungsvorgänge und die Daten, die auf dem Nutzermedium gespeichert werden verständlich für die Kunden beschrieben werden. Soweit es sich bei den Kundenmedien um Chipkarten handelt, die den Bedingungen des § 3 Abs. 10 BDSG entsprechen, hat dieses Informationspapier ferner alle Informationen zu enthalten, die in § 6c Abs. 1 BDSG aufgezählt sind.

   Ferner müssen dann auch die Maßnahmen getroffen werden, die zur Erfüllung von § 6c Abs. 2 und 3 BDSG nötig sind. Dies gilt insbesondere für Absatz 2 (Bereitstellung von Lesegeräten zur Umsetzung des Auskunftsrechts), da Abs. 3 per se erfüllt sein dürfte.

2. Die Kundenvertragspartner sind verpflichtet, den Kunden bei Vertragsabschluss die Möglichkeit zu geben, sich schriftlich dazu zu erklären, ob sie der Übermittlung und Nutzung der Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung zustimmen möchten oder nicht. Sie haben sicherzustellen, dass auch autorisierte Dritte diese Beschränkung beachten.

3. Die Kundenvertragspartner haben die Kunden darüber aufzuklären, welche Möglichkeiten der anonymen Bezahlung und Nutzung der Verkehrssysteme zur Verfügung stehen.

4. Zur Erfüllung des Gebots zur Datenvermeidung und zur Datensparsamkeit (§ 3 a BDSG) werden bei nicht-anonymer Nutzungsweise die für die Abrechnung erforderlichen Daten, die Stammdaten der Kunden und die ansonsten über die Fahrt erhobenen Daten getrennt verarbeitet. Die zu Zwecken der Statistik, zu Planungszwecken und zur Optimierung von Reiseangeboten dienenden Daten werden ohne jeden Bezug zur Person des Kunden gespeichert und weiterverarbeitet. Die Kundenstammdaten und die Rechnungsdaten werden nur zum Zwecke der Abrechnung oder Reklamationsbearbeitung zusammengebracht.

5. Zwischen den EFM-Systembetreibern dürfen nur pseudonyme Daten (auf die Berechtigung bezogene Daten) zu Abrechnungszwecken ausgetauscht werden. Bei nicht-anonymer Nutzungsweise darf nur der Kundenvertragspartner, der mit dem Kunden den „Antrag auf

Ausgabe einer eTicket-Karte (Nutzermedium)“ geschlossen hat, mit schriftlichem Einverständnis des Kunden auf die Kundenidentität zurückgreifen können.
Auf personenbezogene Daten, die auf dem Nutzermedium gespeichert sind, kann ein autorisiertest Terminal nur nach PIN-Eingabe oder asymmetrischer Authentisierung auf diese Daten zugreifen

6. Soweit nicht gesetzliche Aufbewahrungsfristen für personenbezogene oder pseudonyme Abrechnungsdaten bestehen, sind alle bei einer Fahrt entstandenen personenbezogenen oder pseudonymen Daten durch die EFM-Betreiber bzw. Kundenvertragspartner zu löschen oder vollständig zu anonymisieren.

7. EFM-Betreiber und Kundenvertragspartner haben dafür Sorge zu tragen, dass
   - bei der Nutzung von Terminals für die bargeldlose Zahlung Unbefugte daran gehindert werden, die Eingabedaten, vor allem die Authentisierungsdaten zur Kenntnis zu nehmen,
   - Fehlermeldungen an Zugangserfassungssystemen nicht so signalisiert werden, dass die Betroffenen öffentlich diskriminiert werden können,
   - Fehlermeldungen an der Kundenschnittstelle nicht den Grund für den Fehler offenbaren können,
   - Fahrgäste in angemessener Weise die Möglichkeit erhalten, den Inhalt der Chipkarte jederzeit auslesen zu können (§ 6c Abs. 2 BDSG).

8. Im Rahmen einer Vorabkontrolle prüfen die betrieblichen Datenschutzbeauftragten der EFM-Betreiber und der Kundenvertragspartner (Verkehrsbetriebe), ob die unter 1. – 7. beschriebenen Anforderungen erfüllt werden und ob die in der VDV-Kernapplikation spezifizierten technischen und organisatorischen Maßnahmen zur Absicherung der Kundenmedien gegen unbefugte Datenzugriffe (z. B. beim Zugriff durch Kontrollpersonal, bei Verlust) zuverlässig umgesetzt worden sind.

   Die Vorabkontrolle ist für Revisionszwecke (z. B. durch die zuständigen Datenschutzkontrollbehörden) zu dokumentieren.

Auszug aus dem Regelwerk der VDV-Kernapplikation

Kapitel 6: Datenschutz-Grundsätze

1. Die Teilnehmer sind auch gegenüber der VDV-KA KG verpflichtet, die in diesem Kapitel festgelegten Datenschutz-Grundsätze einzuhalten. Im Falle einer nicht-anonymen Nutzung des NM haben die Teilnehmer sicherzustellen, dass die für die Abrechnung erforderlichen Daten, die Stammdaten der Nutzer und Kunden von den ansonsten über die Fahrt erhobenen Daten den datenschutzrechtlichen Vorschriften entsprechend zugriffssicher getrennt gespeichert und verarbeitet werden. Die zu Zwecken der Statistik, zu Planungszwecken und zur Optimierung von Reiseangeboten dienenden Daten dürfen nur ohne jeden Bezug zur Person des Nutzers bzw. des Kunden gespeichert und weiterverarbeitet werden. Das Erstellen personenbezogener Bewegungsprofile ist unzulässig. Die Kundenstammdaten und die Rechnungsdaten dürfen ausschließlich zum Zwecke der Abrechnung oder Reklamationsbearbeitung zusammengeführt werden.

2. Zwischen den Teilnehmern dürfen nur pseudonyme Daten (auf die (((eBezahlberechtigungen bezogene Daten) zu Abrechnungszwecken ausgetauscht werden. Bei nicht-anonymer Nutzung des NM darf grundsätzlich nur der KVP, der mit dem Kunden den Kundenvertrag geschlossen hat, mit Einverständnis des Kunden auf die Kundenidentität zurückgreifen. Nur auf ausdrücklichen Wunsch und Veranlassung des Kunden dürfen auch andere KVP´s auf die Kundendaten zugreifen.

3. Jeder Teilnehmer hat sicherzustellen, dass auf personenbezogene Daten, die auf dem NM gespeichert sind, ein autorisiertes Terminal nur nach PIN-Eingabe oder asymmetrischer Authentisierung zugreifen kann. Auf im Hintergrundsystem (HGS) gespeicherte Daten ist autorisierten Mitarbeitern der Teilnehmer im Rahmen ihrer Tätigkeit im erforderlichen Umfang der Zugriff ohne PIN-Eingabe oder asymmetrischer Authentisierung zu ermöglichen. Für Auskünfte aus dem HGS, die an kundenbedienten Terminals erteilt werden, ist eine PIN-Autorisierung sicherzustellen.

4. Die Teilnehmer haben dafür Sorge zu tragen,

   - dass Fehlermeldungen an Kundenschnittstellen zu (((eTicket-Systemkomponenten nicht so signalisiert werden, dass die Betroffenen öffentlich diskreditiert werden können

     und,

   - dass Fehlermeldungen an der Kundenschnittstelle nicht den ursächlichen Grund für die Fehlermeldung, bzw. die Sperrung (z.B. Säumnis, Vertragsbeendigung, Diebstahl, u.a.) offenbaren können.

5. Soweit nicht gesetzliche Aufbewahrungsfristen für personenbezogene oder pseudonyme Abrechnungsdaten bestehen, oder es zur Bearbeitung von Reklamationen oder zur Geltendmachung von Rechten erforderlich ist, haben die Teilnehmer alle bei einer Fahrt entstandenen personenbezogenen oder pseudonymen Daten nach Wegfall des Aufbewahrungszwecks unverzüglich zu löschen oder vollständig zu anonymisieren. Aufstellungen von Einzelfahrten dürfen nur so lange aufbewahrt werden, wie sie zur Verfolgung von Reklamationen erforderlich sind.

Gilt nur für Teilnehmer in der Rolle des KVP

6. Die von der VDV-KA KG zur Verfügung gestellten Muster-Kundenverträge nebst Allgemeinen Geschäftsbedingungen (**Anlage 3 zum (((eTicket-Teilnahmevertrag**) sind datenschutzrechtlich geprüft und mit Datenschutzbeauftragten abgestimmt worden. Der Teilnehmer ist berechtigt, die Klauseln des Mustervertrages für eigene Zwecke zu verwenden. Die Teilnehmer sind verpflichtet, den Kunden über die Erhebung, Speicherung und Verarbeitung seiner Daten sowie über die dem Kunden zustehenden Widerspruchsrechte sowie Folgen des Widerspruchs zu informieren. Die VDV-KA KG stellt dazu die in der **Anlage 4 zum (((eTicket-Teilnahmevertrag** beigefügten Muster-Datenschutzhinweise zur Verfügung, welche der Teilnehmer dem Kunden vor der erstmaligen Bereitstellung eines (((eTicket-Produktes aushändigen kann.

7. Jeder Nutzer und jeder Kunde hat einen gesetzlichen Anspruch darauf zu erfahren, welche personenbezogenen Daten auf seinem NM und im Hintergrundsystem des KVP gespeichert sind und zu welchen Zwecken diese Daten verarbeitet werden. Die Teilnehmer haben dafür Sorge zu tragen, dass die zur Wahrnehmung dieses Auskunftsanspruchs erforderlichen technischen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

8. Die Teilnehmer sind verpflichtet, jedem Kunden bei Abschluss des Kundenvertrages die Möglichkeit zu geben, sich schriftlich dazu zu erklären, ob er der Übermittlung und Nutzung personenbezogener Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung zustimmen möchte oder nicht. Die Teilnehmer haben darüber hinaus sicherzustellen, dass alle in die Verarbeitung personenbezogener Daten involvierte Stellen diese Beschränkung beachten.

9. Die Teilnehmer haben jeden Kunden darüber aufzuklären, welche Möglichkeiten der anonymen Bezahlung und Nutzung des NM zur Verfügung stehen. Es ist zumindest eine anonym nutzbare Form der Fahrberechtigung bereit zu stellen. Diese muss nicht zwingend in elektronischer Form vorliegen, sondern kann auch im herkömmlichen Papierfahrschein gesehen werden.

10. Die Teilnehmer haben dafür Sorge zu tragen, dass
    - bei der Nutzung von Terminals für die bargeldlose Zahlung Unbefugte daran gehindert werden, die Eingabedaten, vor allem die Authentisierungsdaten zur Kenntnis zu nehmen und
    - Fahrgäste in angemessener Weise die Möglichkeit erhalten, den Inhalt des NM auslesen zu können (§ 6c Abs. 2 BDSG).

- das Personal des Teilnehmers, welcher personenbezogene Daten erhebt, verarbeitet oder nutzt, zur Einhaltung der anwendbaren datenschutzrechtlichen Anforderungen, insbesondere auf das Datengeheimnis nach § 5 BDSG, zu verpflichten.

11. Im Rahmen einer Vorabkontrolle (§ 4d Abs. 5, 6 BDSG) haben die betrieblichen Datenschutzbeauftragten der Teilnehmer zu prüfen, ob die unter Ziff. 1. – 10. beschriebenen Anforderungen erfüllt werden und ob die in der VDV-KA-Dokumentation spezifizierten technischen und organisatorischen Maßnahmen zur Absicherung der Nutzermedien gegen unbefugte Datenzugriffe (z. B. beim Zugriff durch Kontrollpersonal, bei Verlust) zuverlässig umgesetzt worden sind. Die Vorabkontrolle ist für Revisionszwecke (z. B. durch die zuständigen Datenschutzkontrollbehörden) zu dokumentieren.

Anlage

Das Schreiben der berichterstattenden Datenschutzbeauftragten NRW vom 30. Oktober 2012 zum Abschluss der Abstimmungen zwischen den Datenschutzaufsichtsbehörden und dem (((eTicket Deutschland (auf der folgenden Seite).

Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

VDV-Kernapplikations GmbH & Co. KG
Kamekestraße 37-39
50672 Köln

Aktenzeichen
bei Antwort bitte angeben
57.6.2.2

Frau Schonebeck
Telefon 0211 38424-59
Fax 0211 38424-10

eTicket Deutschland
Ihre E-Mail vom 08.08.12

Sehr geehrter Herr Hoffmann,

vielen Dank für die Übersendung der geänderten Vertragsunterlagen. Diese habe ich an die übrigen Datenschutzaufsichtsbehörden mit der Bitte um Stellungnahme weitergeleitet. Hierzu gab es keine weiteren Anmerkungen. Die Abstimmung unter den Datenschutzaufsichtsbehörden ist somit aus meiner Sicht abgeschlossen.

Ich wäre Ihnen dankbar, wenn Sie den LDI NRW über weitere Entwicklungen, die datenschutzrechtliche Aspekte betreffen, informieren würden.

Für Fragen stehe ich gern zur Verfügung und verbleibe
mit freundlichen Grüßen
Im Auftrag

(Schonebeck)

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

Herausgeber:

VDV eTicket Service GmbH & Co. KG
Hohenzollernring 103

D-50672 Köln

Tel.: 49 221 716174 0
Fax: 49 221 716174 123