eTicket Service

# Teilnehmerbrief 1-2018

# Update Datenschutz

## Applikationslogbuch, Unbefugtes Auslesen, Abstimmung mit Landesdatenschutzbeauftragten

## Neue Rechtslage nach Inkrafttreten der EU- Datenschutzgrundverordnung

Datum: 24. Januar 2018

Autor: [redacted]

# Inhaltsverzeichnis

# Editorial

Sehr geehrte Teilnehmer an (((eTicket Deutschland,

dem Datenschutz wird bei (((eTicket Deutschland weiterhin ein besonders hoher Stellenwert zugeschrieben. Die Fahrgäste sind bei diesem Thema jedenfalls in Bezug auf die ÖPV-Nutzung sehr daran interessiert, dass sich die Verkehrsunternehmen und –verbünde (VU/VV) im Umgang mit Kunden- und Transaktionssdaten datenschutzrechtlich konform verhalten.

Die datenschutzrechtlichen Grundanforderungen für das elektronische Fahrgeldmanagement in Deutschland wurden zwischen 2008 und 2012 mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entwickelt und abgestimmt. Das Ergebnis dieser Abstimmung haben wir Ihnen im Teilnehmerbrief Datenschutz vom 22.12.2014 bereits aufbereitet zukommen lassen. Die dort vereinbarten Maßnahmen stellen die konkrete Umsetzung der entsprechenden Regelungen des Bundesdatenschutzgesetzes (BDSG) dar und sind damit die geltende Rechtsgrundlage für die Umsetzung von (((eTicket-Projekten. Die Ergebnisse sind daher auch in das (((eTicket-Regelwerk und die Feinspezifikationen der VDV-Kernapplikation eingeflossen.

Dieser Teilnehmerbrief soll Sie zum einen über die aktuellen Entwicklungen im Zusammenhang mit dem Applikationslogbuch (auch Kontroll- oder Transaktionsspeicher genannt) auf der Chipkarte informieren. Diese mit den Aufsichtsbehörden von Anfang an abgestimmte Funktionalität wird immer wieder von einzelnen Bürgern zumeist medienwirksam in der Lokalpresse als datenschutzrechtlich bedenklich kritisiert. Der VDV eTicket Service hat dazu eine erneute Abstimmung mit den Aufsichtsbehörden gesucht und sich die datenschutzrechtliche Unbedenklichkeit bestätigen lassen.

Des Weiteren treten am 25.05.2018 die EU-Datenschutzgrundverordnung (DSGVO) und auch das neue Bundesdatenschutzgesetz (BDSG neu) in Kraft. Damit erhält das Datenschutzrecht eine völlig neue Rechtsgrundlage. Dieser Teilnehmerbrief soll einen Überblick über die wichtigsten Änderungen geben. Die konkreten Auswirkungen und Anforderungen auf (((eTicket-Systeme sind noch nicht klar umrissen und werden es wohl auf absehbare Zeit auch nicht sein. Wir haben daher eine Abstimmung mit den Aufsichtsbehörden vorgenommen, über die wir Sie in diesem Teilnehmerbrief ebenfalls unterrichten möchten. Darin enthalten ist auch eine Handlungsempfehlung des zuständigen Landesdatenschutzbeauftragten, wie man sich verhalten soll, um dem neuen Datenschutzrecht zu entsprechen.

[redacted]

VDV eTicket Service GmbH & Co. KG

# I. Applikationslogbuch

Die Funktion des Applikationslogbuchs 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. Damit wird der datenschutzrechtliche Grundsatz der Transparenz erfüllt, der u.a. beinhaltet, dass der Kunde den Inhalt seiner Karte bzw. die Datenübertragungsvorgänge, die von der Karte elektronisch getätigt wurden, jederzeit auslesen können muss. Je nach Ausbaustufe Ihres (((eTicket Deutschland Systems können dies reine Kontrolleinträge sein (Zeitpunkt der Fahrausweiskontrolle und chiffrierte Ortskennung) oder tatsächliche Ticketkäufe und damit ein digitaler Kundenbeleg für Reklamationen. Als Kontrolleinträge sind diese vergleichbar mit dem Stempel der Fahrkartenentwerter oder einer Quittung bei Papiertickets. Auch die Aufladung eines Prepaid-Kontos auf der Karte wird angezeigt. Mit dem Auslesen des Applikationslogbuches kann der Fahrgast also beispielsweise überprüfen, ob das von ihm eingezahlte Guthaben auch tatsächlich im Werteinheitenspeicher der Karte gutschrieben wurde oder ob das gekaufte Ticket tatsächlich auf seiner Karte gespeichert worden ist.

Dieses Verfahren ist mit den Datenschutzaufsichtsbehörden abgestimmt und im Sinne der Datensparsamkeit auf zehn Einträge begrenzt. Eine neu hinzukommende Transaktion überschreibt dann die jeweils Älteste der 10 zuvor gespeicherten Transaktionen wieder.

Diese Transaktionen werden auch an das für die genutzte Fahrtberechtigung zuständige Hintergrundsystem weitergeleitet. 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 durchzuführen.

# 1. Kritik am Applikationslogbuch

Den Verkehrsunternehmen gegenüber wurde bereits mehrfach unterstellt, mit dem Applikationslogbuch Daten sammeln zu wollen, um Bewegungsprofile der Kunden erstellen zu können. Erstmals wurden diese Vorwürfe im Dezember 2015 in Berlin erhoben[1].
Derartige Vorwürfe sind selbstverständlich völlig unbegründet. Die Lokalpresse neigt in derartigen Fällen jedoch gerne dazu, die Berichterstattung zu dramatisieren („Datenklau“, „Spionage“, „Datenleck“), obwohl es dazu in keinem Fall Anhaltspunkte gab.
Es besteht Einigkeit mit den Aufsichtsbehörden, dass die Bildung eines Bewegungsprofils von der Dichte der Fahrscheinkontrollen abhängt und die Kontrollhäufigkeit daher in eine Risikobetrachtung einfließen muss. Die aktuelle Kontrolldichte bei sporadischen Fahrausweisprüfungen wird nicht als kritisch angesehen, da sich daraus keine aussagekräftigen Bewegungsprofile ableiten ließen.

Die datenschutzrechtlichen Aspekte um den Applikationslogbucheintrag wurden seitens der Aufsichtsbehörden bereits bei Einführung des (((eTicket Deutschland und in jüngerer Vergangenheit erneut auf datenschutzrechtliche Konformität überprüft, mit dem Ergebnis, dass dieser nicht zu beanstanden ist. Sämtlichen datenschutzrechtlichen Grundsätzen, insbesondere auch dem der Datensparsamkeit, wird mit der umgesetzten Funktionalität Rechnung getragen.

Die Nutzung des Applikationslogbuchs wird seit Bestehen von (((eTicket Deutschland in weiten Teilen Deutschlands praktiziert und von allen zuständigen Landesdatenschutzbehörden akzeptiert. Mit Zunahme von NFC-fähigen Smartphones wächst auch die Möglichkeit der Fahrgäste, mit Hilfe von passenden Apps (die sich aktuell eher an Entwickler richten), ihre eigene Chipkarte auszulesen. Es empfiehlt sich, das Auslesen der Chipkarte als bewusste Servicefunktion in der App des eigenen Verkehrsunternehmens bzw. –verbundes anzubieten.

Wichtig ist in diesem Zusammenhang, dass der Kunde bei Abschluss des (((eTicket-Vertrags in den Datenschutzhinweisen innerhalb der AGB über die Speicherung der jeweils letzten 10 Transaktionen auf seiner Chipkarte informiert wird. Der VDV eTicket Service stellt hierfür entsprechende Muster zur Verfügung[2].

[1] Vgl. eTicket Deutschland Hintergrundinformationen „Angebliches Datenleck bei VBB-Fahrcard“; Ihnen durch den VDV eTicket Service zugesandt am 05. Januar 2016
[2] Siehe Anlage 4 (((eTicket-Regelwerk „Muster Datenschutzhinweise“ V1.25.

## 2. Unbefugtes Auslesen der Chipkarte

Regelmäßig wird im Zusammenhang mit der Kritik am Applikationslogbuch auch der Vorwurf erhoben, dass ein (((eTicket auch jederzeit mit dem Smartphone eines unbefugten Dritten sozusagen „im Vorbeigehen“ ausgelesen werden könnte.

In einer Sitzung mit den Datenschutzaufsichtsbehörden im Juli 2017 wurde einvernehmlich festgestellt und protokolliert, dass ein Auslesen der bei (((eTicket Deutschland verwendeten Chipkarten durch unbefugte Dritte mittels eines NFC-Handys in der Praxis nahezu unmöglich ist. Die Karte muss für mehrere Sekunden unmittelbar und ohne Bewegung an das Telefon gehalten werden. Das ist unbemerkt kaum möglich. Wenn sich Kleidung oder ein Portemonnaie zwischen Karte und Lesegerät befinden, findet ebenfalls kein Datenempfang statt. Die Gefahr eines unbefugten Auslesens einer in einem Portemonnaie zusammen mit anderen Karten befindlichen Chipkarte wird daher als theoretisch eingestuft. Wenn einzelnen Kunden das verbleibende minimale Restrisiko zu groß ist, können sie die Chipkarte in einer Funk-Schutzhülle aufbewahren, die jegliche kontaktlose Übertragung verhindert. Derartige Schutzhüllen könnten den Kunden vom VU/VV auf Wunsch ggf. auch zur Verfügung gestellt werden.

Grundsätzlich kann der Vorwurf der Möglichkeit eines unbefugten Auslesens jedoch mit o.g. Begründung zurückgewiesen werden.

## 3. Persönliche Daten in der Fahrtberechtigung

Grundsätzlich werden Personenstammdaten nicht auf der Chipkarte, sondern im Hintergrundsystem des Kundenvertragspartners (also bei dem Verkehrsunternehmen, der seinem Kunden die Chipkarte ausgibt) und damit geschützt vor jeglichem fremden Zugriff gespeichert.

Im Falle eines personalisierten Tickets werden die zur Kontrolle erforderlichen Daten (Name, Geburtsdatum, Geschlecht) jedoch auch innerhalb der Berechtigung, also dem auf der Karte liegenden elektronischen Ticket gespeichert. Ansonsten wäre eine Zuordnung der Fahrtberechtigung zur tatsächlich fahrtberechtigten Person nicht möglich. Rabattierte Tickets (Schüler-, Studenten-, Senioren-, Jobtickets, etc.) existieren i.d.R. nur personalisiert.

Würden diese nicht personalisiert ausgegeben, wären diese übertragbar und könnten von Personen genutzt werden die die Kriterien eines vergünstigten Fahrpreises nicht erfüllen.

Das Auslesen der Berechtigung ist mit einem NFC-fähigen Smartphone und einer entsprechenden kostenlosen App (bspw. „mytraQ“ oder „NFC TagInfo“) möglich.

Dass VU/VV bislang teilweise darauf verzichten, regelmäßig bei der Kontrolle alle Identifizierungsmerkmale zu überprüfen, liegt in deren Ermessen. Aus diesem Umstand kann man aber keine Rückschlüsse auf die datenschutzrechtliche Zulässigkeit der Speicherung von Identifikationsmerkmalen in einem (((eTicket schließen. Es sollte unstrittig sein, dass das Verkehrsunternehmen die Möglichkeit haben muss, bei personengebundenen Tickets die Identität des Fahrgastes zweifelsfrei feststellen zu können. Diese Sicht teilen auch die Datenschutzaufsichtsbehörden.

Eine Speicherung der zur Identifikation erforderlichen persönlichen Daten in der Berechtigung hat demnach einen datenschutzrechtlich legitimen Zweck. Kunden, die dies nicht möchten, müssen die Möglichkeit haben, ein anonymes, nicht personengebundenes Tarifprodukt erwerben zu können. Einen Anspruch auf eine vergleichbare Rabattierung der anonymen Tarifprodukte hat der Kunde in derartigen Fällen jedoch nicht.

# 4. Erfolgte Abstimmung mit Aufsichtsbehörden

Mit den Datenschutz-Aufsichtsbehörden wurde am 26. Juli 2017 vereinbart, dass die Applikationslogbuch-Problematik zu lösen ist, indem den Kunden Möglichkeiten der Löschung von Applikationslogbuch-Einträgen auf der Chipkarte an Terminals in Servicecentern der Verkehrsunternehmen und- verbünde (VU/VV) geschaffen werden. Diese Möglichkeiten sind bereits von Beginn an in der VDV-Kernapplikation vorgesehen. Informationen über die Löschungsmöglichkeit allgemein, sowie wo und wie diese durchzuführen ist, müssen die VU/VV in die Beförderungsbedingungen aufnehmen. Für bereits bestehende Vertragsverhältnisse sollte eine entsprechende Information an die Kunden über die Website des VU/VV erfolgen.

Dies müsse jedoch deutlich sichtbar für die Kunden erfolgen (z.B. auf der Startseite im Internetauftritt des Verkehrsunternehmens oder bei den Informationen zum entsprechenden Tarifprodukt), damit die Kunden auch tatsächlich von der Option der Löschung von Einträgen auf der Chipkarte Kenntnis erlangen. Ein Hinweis auf diese Option z.B. nur im FAQ-Bereich ist nicht ausreichend, da dies die Gefahr bietet, dass viele Kunden dann davon keine Kenntnis erlangen und dementsprechend dieses Recht nicht wahrnehmen (können).

Mit der Feststellung, dass unbefugtes Auslesen einer in einem Portemonnaie zusammen mit anderen Chipkarten befindlichen VDV-KA-konformen Chipkarte als eher

unwahrscheinlich anzusehen ist und dass die Kunden über die Löschungsmöglichkeit des Applikationslogbuchs informiert werden sollen, sehen die Datenschutz-Aufsichtsbehörden die Problematik um das Applikationslogbuch als gelöst an, sobald die Löschungsmöglichkeit aktiv kommuniziert wurde und auch tatsächlich den Kunden zur Verfügung steht.

Sollten sich bei Ihnen Fahrgäste oder die Lokalpresse zu diesem Thema melden, können Sie diese gerne an den VDV eTicket Service, Ansprechpartner Herr Ackers oder Herr Hoffmann, verweisen. Wir können auch Antworten auf entsprechende Fragen und vorgefertigte Pressemitteilungen zur Verfügung stellen.

Das als Anlage beigefügte Dokument „Kontrollnachweise EFS“ erläutert in detaillierter Form die Notwendigkeit der Erzeugung von Kontrollnachweisen bei elektronischen Fahrscheinen zu Sicherheitszwecken. Es bietet eine Unterstützung der VU/VV bei der Erstellung eines Datennutzungskonzeptes und kann auch als Grundlage für die Beantwortung kritischer Fragen seitens der Öffentlichkeit (Presse, Kunden,...) helfen. Darüber hinaus mag es als Unterstützung der VU/VV dienen, um die im Teilnehmerbrief erwähnten Anforderungen zu erfüllen.

# II. Das neue Datenschutzrecht

## 1. Rechtsquellen

Das Datenschutzrecht hat nach 4-jährigen Verhandlungen auf EU-Ebene eine umfassende strukturelle Reform erlebt.
Die neuen Rechtsquellen sind:

- EU-Datenschutzgrundverordnung (DSGVO)
- Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)
- Bundesdatenschutzgesetz (BDSG neu)

## 2. Die Datenschutzgrundverordnung (DSGVO)

Diese gilt unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018 und zwar erstmals auch für Unternehmen, die ihren Sitz nicht in der EU haben, aber in der EU auf Bürger „einwirken“, d.h. in der EU geschäftlich tätig sind (sog. Marktortprinzip).

Mit der Einführung der DSGVO sollen die Datenverarbeitungsregeln EU-weit vereinheitlicht werden und Datenschutz soll zur „Chefsache“ werden. Ob diese beiden erklärten Ziele erreichbar sind, darf bezweifelt werden; es besteht aber Grund zur Annahme, dass mit dem neuen Datenschutzrecht ein stärkeres Bewusstsein für datenschutzrechtliche Erfordernisse in der Wirtschaft geschaffen werden kann, was angesichts der „Datensammelwut“ insbesondere einiger amerikanischer Unternehmen grundsätzlich zu begrüßen ist.

Die DSGVO ergänzt grundsätzlich die Betroffenenrechte (z.B. Recht auf Vergessen, Datenportabilität, Intervenierbarkeit des Kunden) und sie stärkt auch die Möglichkeiten der Geltendmachung von Schadensersatz, was bislang häufig schwierig war.

Generell verpflichtet die DSGVO zu gewissenhafteren Umgang mit Daten. Insbesondere treffen die Unternehmen deutlich verschärfte Dokumentationspflichten. Ein Unternehmen muss die Einhaltung der DS-Vorschriften zukünftig nachweisen können.

In der DSGVO sind ca. 50 Öffnungsklauseln für nationale Datenschutzgesetze (in Deutschland: BDSG neu) enthalten. Letztlich muss daher in allen Fällen, in denen die

DSGVO eine detailliertere Regelung durch die nationale Gesetzgebung vorsieht, wieder der Blick in das jeweilige Datenschutzgesetz des Mitgliedsstaates fallen, in dem man gerade tätig ist. Hierdurch dürfte das Ziel der europaweiten Vereinheitlichung zumindest teilweise konterkariert werden, da die nationale Gesetzgebung in den Mitgliedstaaten häufig stark voneinander abweicht.

## 3. Das neue Bundesdatenschutzgesetz

In Deutschland wurde im Rahmen des Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) auch das neue Bundesdatenschutzgesetz am 12.05.2017 beschlossen und am 05.07.2017 im Bundesgesetzblatt veröffentlich. Es entfaltet seine Geltung ab dem 25.05.2018.

Das BDSG n.F. regelt spezielle Bereiche des nationalen Datenschutzrechts auf der Basis der DSGVO (Lückenfüllung bzw. Konkretisierung bei o.g. Öffnungsklauseln).

Grundsätzlich haben die Regelungen der DSGVO Vorrang (§ 1 V BDSG neu). Das BDSG neu ist nur Ergänzung zur DSGVO. Das BDSG neu ist in der Ausfüllung der Öffnungsklauseln teilweise strenger als die DSGVO selbst (z.B. Bestellung eines Datenschutzbeauftragten, § 38 BDSG neu).

## 4. Konsequenzen für Verkehrsunternehmen und –Verbünde

Die DSGVO enthält (naturgemäß) abstrakte und nicht konkret auf EFM-Systeme bezogene Regelungen. Die konkrete Umsetzung der DSGVO in der Verkehrsbranche bzw. in Bezug auf (((eTicket-Systeme ist daher noch nicht klar umrissen. Der VDV eTicket Service hat seit Verabschiedung der DSGVO im Jahr 2016 bei den Datenschutzaufsichtsbehörden um eine Konkretisierung bzw. um konkrete Handlungsanweisungen gebeten. Die Aufsichtsbehörden geben jedoch trotz Anfrage keine konkreten Empfehlungen, man beantwortet dort aber konkrete Fragen des Einzelfalls. Bis der Umfang der Geltung einzelner Bestimmungen von DSGVO und BDSG neu für die Anwender durch eine einheitliche Verwaltungspraxis rechtssicher bestimmt ist, werden wohl noch einige Jahre vergehen. Nichtsdestotrotz sind die DSGVO und das BDSG neu in Kraft und demnach einzuhalten.

Eine Neubewertung der VDV-Kernapplikation aufgrund der neuen Rechtslage ist jedenfalls nach Auskunft der Datenschutzbehörden ausdrücklich nicht geplant.

# 5. Datenschutzfolgeabschätzung (DSFA), Art. 35 DSGVO

Sämtliche VU/VV, die an (((eTicket Deutschland teilnehmen, sind nach DSGVO verpflichtet, eine DSFA durchzuführen. Eine üblicherweise zuvor durchzuführende Schwellwertanalyse (Art. 35 III DSGVO) ist laut der zuständigen Datenschutz-aufsichtsbehörde nicht erforderlich, da das Ergebnis bereits feststeht. Ggf. ist eine Muster-DSFA für alle (((eTicket-Betreiber auf Basis einer von einem VU/VV bereits durchgeführten DSFA möglich.

In den Abstimmungen mit den Datenschutzaufsichtsbehörden wurde jedoch eine Alternative aufgezeigt, die eine Durchführung einer DSFA nicht erforderlich macht und deren Umsetzung der VDV eTicket Service empfiehlt:

Eine mögliche Auslegung der DSGVO für die neue Auffassung der europäischen Datenschutzaufsichtsbehörden (im Working Paper 248 der Art. 29 Gruppe[3]) in Bezug auf die Durchführung einer DSFA ist, dass bei Bestandsverfahren (darunter fällt (((eTicket Deutschland) auf eine DSFA ausnahmsweise dann verzichtet werden kann, wenn eine vollständige und dokumentierte Vorabkontrolle nach § 4d Abs. 5 BDSG durch den Beauftragten für den Datenschutz durchgeführt wurde und das Risiko nicht wesentlich verändert ist. (LDI NRW, Az. 57.6.2.2 – 3899/17).

**Die VU/VV sollten daher –sofern nicht bereits erfolgt- eine entsprechende Vorabkontrolle nach altem Recht bis 25.05.2018 durchgeführt und entsprechend dokumentiert haben.**

Im Rahmen einer Vorabkontrolle prüfen die betrieblichen Datenschutzbeauftragten, ob die datenschutzrechtlichen Anforderungen[4] erfüllt werden und ob die in der VDV-Kernapplikation spezifizierten technischen und organisatorischen Maßnahmen zur Absicherung der Kundenmedien gegen unbefugte Datenzugriffe zuverlässig umgesetzt worden sind.

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

Bereits in den geltenden (((eTicket-Teilnahmeverträgen werden die Teilnehmer auf die grundsätzliche Verpflichtung der Vorabkontrolle hingewiesen („Von dem oder der

[3] Die Artikel-29-Datenschutzgruppe, engl. Article 29 Data Protection Working Party, teilw. mit „G29“ abgekürzt, ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes.
[4] Die Anforderungen sind enthalten im Teilnehmerbrief „Datenschutz“ vom 22.12.2014, der beim VDV eTicket-Service gerne erneut zur Verfügung gestellt wird.

betrieblichen Datenschutzbeauftragten ist vor Inbetriebnahme des (((eTicket-Systems eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG alt) und zu dokumentieren“).

Im Zweifel ist eine Abstimmung mit Ihrem Landesdatenschutzbeauftragten (LDI) ratsam. Bitte weisen Sie Ihren LDI darauf hin, dass ein Großteil der notwendigen Abstimmung – soweit abstrakt möglich- bereits erfolgt ist. Auf den Alternativvorschlag zur Durchführung einer DSFA seitens des LDI NRW (Az. 57.6.2.2-3899/17) sollten Sie ebenfalls hinweisen, wenn Sie sich für diese Variante entscheiden.

## 6. Transparenz

Aus der DSGVO ergeben sich umfangreichere Dokumentations- und Informationspflichten. Fest steht, dass alle VU/VV zukünftig ihre sämtlichen Prozesse im Umgang mit Daten auf Risiken im Zusammenhang mit dem Datenschutz analysieren und die Ergebnisse entsprechend dokumentieren müssen. Ggf. wird sich aus dieser Analyse auch bereits konkreter Handlungsbedarf ergeben. Die Dokumentation ist jedoch auch durchzuführen und aufzubewahren, wenn kein Handlungsbedarf festgestellt wird. Die Dokumentation muss also auch Auskunft darüber geben, warum man bestimmte datenschutzrechtliche Vorkehrungen nicht trifft und die Gründe dafür sind zu nennen. Letztlich muss dokumentiert sein, dass sämtliche Risiken betrachtet worden sind. Hierzu wollen die Datenschutzaufsichtsbehörden Checklisten und Muster bereitstellen.

Art. 5 Abs. 1 a) DSGVO fordert: „Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‚Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz‘)“.

Gegenüber Betroffenen sind zudem die Art. 12 ff. DSGVO zu erfüllen. Alle diese Anforderungen müssen im Rahmen der Risikoanalyse für jeden datenschutzrechtlich relevanten Prozess überprüft werden.

Daraus folgt, dass der Verantwortliche sich zuerst selbst einen umfassenden Überblick über die Verarbeitungsvorgänge verschaffen muss und dann den Betroffenen daraus eine verständliche, nachvollziehbare Information zur Verfügung stellen muss.

Gegenüber Betroffenen muss die Information nicht in der Tiefe erfolgen, die ein beim Verantwortlichen tätiger Ingenieur, Techniker, Informatiker etc. für notwendig erachten würde, sondern es soll eine Orientierung am Empfängerhorizont erfolgen.

# 7. Sanktionen

Die Möglichkeiten von Sanktionierungen bei Verstößen gegen das Datenschutzrecht sind zweifellos erheblich verschärft worden. Die DSGVO enthält deutlich strengere Sanktionen bei Verstößen gegen die darin niedergelegten Regelungen (Bußgeld in Höhe von bis zu 4 % des Jahresumsatzes oder bis zu 20 Mio. €). Dennoch ist es nicht angebracht, deshalb in Hysterie zu verfallen.
Zu den Sanktionen sind die Aufsichtsbehörden noch im Abstimmungsprozess auf nationaler und europäischer Ebene. Bei der Höhe von Geldbußen wird aber weiterhin der Rechtsgrundsatz der Verhältnismäßigkeit anzuwenden sein.

Daher sind wohl bei einer Geldbuße bspw. für eine verspätete DSFA bei Bestandsverfahren für einen Übergangszeitraum aufgrund der vorherigen anders geplanten Verwaltungspraxis (WP 248) diese Umstände mildernd zu berücksichtigen. Die (((eTicket-Deutschland-Umsetzungen werden von den Datenschutzaufsichtsbehörden als solche Bestandsverfahren angesehen. Darauf sollten Sie Ihren Landesdatenschutzbeauftragten im Falle einer Prüfung hinweisen.

Auch grundsätzlich werden die Geldbußen sich weiterhin an der Schwere des Verstoßes, den Auswirkungen für die Betroffenen, der Erkennbarkeit sowie an der Einsichtsfähigkeit und dem Änderungswillen der Verantwortlichen orientieren.

Die in Art. 83 DSGVO genannten Maximalsummen dürften folglich eher die  Ausnahme bleiben.

# 8. Weiterführende Links:

https://www.lda.bayern.de/de/datenschutz_eu.html

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/KP_10_Informationspflichten.pdf

http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

https://www.bitkom.org/datenschutz/

https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/KP_5_Datenschutz-Folgenabschaetzung.pdf

https://www.bvdnet.de/ds-gvo-wichtige-handlungsfelder-fuer-unternehmen/

Herausgeber:

VDV eTicket Service GmbH & Co. KG
Im Mediapark 8a
50670 Köln

Telefon: +49 221 716174 0
Fax: +49 221 716174 123
E-Mail: info@eticket-deutschland.de
Website: www.eticket-deutschland.de