RHEIN-MAIN-VERKEHRSVERBUND

vHGS-Vertrag

Vertrag
über die
Nutzung, Teilnahme und Zusammenarbeit am
verbundweiten mandantenfähigen Hintergrundsystem
(vHGS) des eTicket RheinMain

zwischen
der

Rhein-Main-Verkehrsverbund GmbH
Alte Bleiche 5
Hofheim am Taunus

- nachstehend auch „RMV“ genannt -

und

.....
.....
.....

- nachstehend auch „Teilnehmer“ genannt -

Thema:	Vertrag über die Nutzung, Teilnahme und Zusammenarbeit am verbundweiten mandanten-fähigen Hintergrundsystem (vHGS) des eTicket RheinMain
Dateiname:	vHGS-Vertrag
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	1.1
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Version zur Vertragsunterzeichnung
1.1	RMV	20.02.2019	Anpassungen an DSGVO und Aufnahme des neuen Aufgabenbereichs „Vertrieb JobTicket ohne Service durch Dritte“

Inhalte

Anlagen

Nachrichtlich:

Präambel

Die Rhein-Main-Verkehrsverbund GmbH (RMV) hat zum Fahrplanwechsel 2011/2012 im RMV-Gebiet mit der flächendeckenden Einführung eines Elektronischen Fahrgeldmanagements (EFM) begonnen und in den letzten Jahren gemeinsam mit den Partnern im RMV auf Basis einer einvernehmlichen Grundlage, vertrauensvoll und erfolgreich umgesetzt.

Als ein kundengerechtes und effizientes Vertriebssystem soll das EFM langfristig die Einnahmen erhöhen und Potentiale zur Kostensenkung schaffen.

Kernelement dieses Vertriebssystems ist das verbundweite Hintergrundsystem (vHGS), welches eine koordinierte Abwicklung aller vertrieblichen Prozesse des EFM ermöglicht und auf dessen Basis die Teilnehmer eine gemeinsame Kundenbetreuung durchführen ("Service durch Dritte") können (ausgenommen der Aufgabenbereich JobTicket).

§ 1 Gegenstand des Vertrages

Gegenstand dieses Vertrages ist die Festlegung von Rechten und Pflichten der Vertragspartner für die Nutzung des vHGS im Tarif-Anwendungsgebiet des RMV.

Die Anlagen 1 bis 12 sind Vertragsbestandteil (ausgenommen Anlage 3, diese gilt nicht für den Aufgabenbereich JobTicket). Im Fall von Widersprüchen gehen die Vereinbarungen zur Auftragsverarbeitung den Regelungen des Vertrages und sonstigen Anlagen vor.

§ 2 Vertragspartner

(1) Zwischen den Vertragspartnern wird durch Abschluss dieses Vertrages kein gesellschaftsrechtliches Verhältnis und hieraus entstehende Rechte und Pflichten begründet, weder zwischen den Teilnehmern untereinander noch zwischen den Teilnehmern und dem RMV.

(2) Voraussetzung zur Teilnahme am vHGS ist der Abschluss dieses Vertrages sowie eines Vertrages über die Teilnahme am (((eTicket-Deutschland „(((eTicket-Teilnahmevertrag“ mit der VDV-Kernapplikations GmbH & Co.KG, Köln (VDV-KA KG). Dabei sind die vom RMV gewählten Migrationsschritte Ausbauvariante 2a gemäß „Vertrag über die Teilnahme am (((eTicket-Deutschland – (((eTicket-Teilnahmevertrag mit dem auf die Rhein-Main-Verkehrsverbund GmbH spezifizierten Migrationsszenario“ (vgl. Anlage 9) Mindestvoraussetzung für den Teilnehmer.

Über den Abschluss des (((eTicket-Teilnahmevertrages des Teilnehmers ist ein Nachweis zu erbringen. Für den Nachweis reicht die Übersendung einer Kopie der ersten und letzten Seite des unterzeichneten Vertrages über die Teilnahme am (((eTicket-Deutschland „(((eTicket-Teilnahmevertrag“, die die Vertragspartner sowie Unterschrift der Beteiligten und Datum erkennen lässt.

§ 3 Aufgaben des RMV

(1) Der RMV übernimmt die in diesem Vertrag benannten Aufgaben. Im vHGS nimmt der RMV die KA-Rolle des Produktverantwortlichen (PV), wie sie sich aus § 1 (((eTicket-Teilnahmevertrag ergibt, ein.

(2) Der RMV ist Eigentümer des vHGS und ist verantwortlich für die fachliche und technische Betriebsführung.

(3) Der RMV stellt das vHGS zur Nutzung durch die Teilnehmer bereit und sorgt für die Abnahme durch einen Wirtschaftsprüfer. Diese Abnahme ist den Teilnehmern vorzulegen. Für den Zeitraum zwischen Betriebsaufnahme und Abnahme durch den Wirtschaftsprüfer obliegt es dem RMV sicherzustellen, dass die Grundsätze ordnungsmäßiger Buchführung, an denen sich ordentliche Kaufleute zu orientieren haben, eingehalten werden.

(4) Der RMV koordiniert die Zusammenarbeit der Teilnehmer im vHGS nach Maßgabe dieses Vertrages und pflegt eine Liste mit allen Teilnehmern am vHGS (vgl. Anlage 7).

(5) Der RMV ist berechtigt zur Erfüllung seiner Leistungen Subunternehmer einzusetzen. Die Teilnehmer werden über die Beauftragung von Subunternehmern sowie deren Namen und Adresse informiert. Die Verantwortung des RMV gegenüber den Teilnehmern für die in diesem Vertrag eingegangenen Pflichten wird durch die Beauftragung von Subunternehmern nicht berührt.

§ 4 Aufgaben des Teilnehmers

(1) Der Teilnehmer übernimmt im vHGS die KA-Rolle des Kundenvertragspartners (KVP) und/oder des Dienstleisters (DL), wie sie sich aus § 1 (((eTicket-Teilnahmevertrag ergibt.

(2) Dem Teilnehmer sind folgende vHGS Aufgabenbereiche zugeordnet:

- o Online vHGS (inkl. Service durch Dritte)
- o Vertrieb JobTicket (ohne Service durch Dritte)
- o Offline vHGS
- o TicketShop
- o Kontrolle

(Der entsprechende vHGS Aufgabenbereich ist anzukreuzen; ein Teilnehmer kann auch mehrere Aufgabenbereiche übernehmen.)

(3) Die Aufgabenbereiche sind näher in Anlage 1 „Regelwerk vHGS“ definiert.

(4) Der Teilnehmer hat für die Einhaltung der Anforderungen aus dem Regelwerk vHGS entsprechend seiner Aufgabenbereiche Sorge zu tragen.

(5) Der Teilnehmer ist berechtigt, zur Erfüllung seiner Leistungen Subunternehmer einzusetzen. Der RMV ist über die Beauftragung sowie Namen und Adressen der Subunternehmer zu informieren. Die Verantwortung des Teilnehmers gegenüber dem RMV für die in diesem Vertrag eingegangenen Pflichten wird durch die Beauftragung von Subunternehmern nicht berührt.

(6) Der Teilnehmer ist ferner berechtigt, auch Vertriebsdienstleister (VDL) einzusetzen, die die Datenverarbeitung selbständig als Verantwortlicher im datenschutzrechtlichen Sinne wahrnehmen und insoweit allein die Verantwortung für die Verarbeitung der Daten und die daraus erwachsenden datenschutzrechtlichen Pflichten, wie z. B. die Wahrnehmung der Rechte gegenüber Betroffenen, tragen.

§ 5 Nutzungsbedingungen vHGS

(1) Allen Teilnehmern werden folgende vHGS-Systemkomponenten ohne Lizenzkosten zur Nutzung gemäß dieses Vertrages zur Verfügung gestellt:
- vHGS,
- Crystal Reports Viewer,
- Kartenleser-Dienstprogramm.

(2) Durch die Teilnahme am vHGS erwerben die Teilnehmer weder vHGS-Systemkomponenten noch Rechte oder Lizenzen daran. Soweit zur Erfüllung ihrer vertraglichen Pflichten gegenüber dem RMV, gegenüber anderen Teilnehmern oder gegenüber den Kunden darüber hinaus Komponenten, Lizenzen oder Rechte erforderlich sind, haben sich die Teilnehmer erforderliche Komponenten, Lizenzen oder Rechte daran zu beschaffen.

(3) Die Nutzung des vHGS ist grundsätzlich nur im Tarif-Anwendungsgebiet des RMV innerhalb der in § 4 (2) festgelegten Aufgabenbereiche gestattet. Eine Nutzung darüber hinaus ist mit dem RMV im Einzelfall abzustimmen.

(4) Die zusätzliche Nutzung eines eigenen Hintergrundsystems/Vertriebssystems ist möglich, soweit hierdurch die Funktionalität des vHGS und die verbundweiten Kontrollprozesse nicht beeinträchtigt werden. Die Voraussetzungen zur Nutzung eines eigenen Hintergrundsystems sind im Regelwerk vHGS beschrieben (vgl. Anlage 1, Kapitel 4.2 erster Fall).

Ist die ergänzende Nutzung eines eigenen Systems vorgesehen, ist der RMV darüber rechtzeitig vor Betriebsstart zu informieren. Es gelten die Rahmenbedingungen der Anlage 6 dieses Vertrages. Hierdurch entstehende zusätzliche Kosten trägt der jeweilige Teilnehmer selbst.

(5) Der RMV oder ein von ihm beauftragter Dritter ist Ansprechpartner für die Belange, die sich aus der Nutzung des vHGS ergeben. Kann das vHGS nicht vertragsgemäß genutzt werden, ist entsprechend Kapitel 2 und 3 des Regelwerks vHGS zu handeln (siehe Anlage 1).

(6) Der Teilnehmer ist berechtigt zur Erfüllung seiner Leistung Subunternehmer einzusetzen.

§ 6 Zuordnung der Verträge aus dem RMV-TicketShop

Die Zuordnung von Kundenverträgen zu den KVP bei Bestellung aus dem RMV-TicketShop erfolgt im vHGS nach Maßgabe der nachfolgend dargestellten Logik:

- Gelangt ein Kunde von einer teilnehmereigenen Webseite zum RMV-TicketShop, erfolgt die Zuordnung des zu schließenden Kundenvertrages zu diesem Teilnehmer.
- Bei einem direkten Zugriff auf den RMV-TicketShop von im RMV-Tarif-Anwendungsgebiet wohnhaften Kunden erfolgt die Zuordnung der Bestellung zu einem KVP nach Postleitzahl (PLZ). Die jeweils zuständige LNO entscheidet, wer die Leistungen aus dem RMV-TicketShop übernimmt und welche PLZ zugeordnet werden.
- Beim Zugriff auf den RMV-TicketShop von außerhalb des RMV-Tarif-Anwendungsgebiets wohnhaften Kunden wird DB Regio AG, Region Hessen Kundenvertragspartner (KVP).

§ 7 Vertragsänderungen

(1) Sollten Änderungen dieses Vertrages erforderlich sein, werden diese den Teilnehmern rechtzeitig, spätestens drei Monate vor Wirksamwerden, schriftlich mitgeteilt.

(2) Vertragsänderungen gelten für den jeweiligen Teilnehmer als genehmigt, sofern dieser nicht innerhalb von sechs Wochen nach Eingang der schriftlichen Nachricht gegen den entsprechenden Änderungsvorschlag schriftlich Einspruch erhebt.
(3) Im Falle eines Einspruchs werden die Vertragsparteien innerhalb der auf den Eingang des Einspruchs folgenden sechs Wochen Verhandlungen über eine einvernehmliche Lösung aufnehmen.
(4) Können sich die Vertragspartner auf eine Vertragsänderung nicht innerhalb dieser Frist einigen, kann der jeweilige Teilnehmer diesen Vertrag innerhalb von zwei weiteren Wochen fristlos kündigen.
(5) Jede beabsichtigte Vertragsänderung ist vorab im entsprechenden Anwenderkreis (vgl. § 8) zu diskutieren.

§ 8 Teilnehmertreffen und Anwenderkreise

(1) Einmal jährlich findet eine Informationsveranstaltung für alle Teilnehmer am vHGS statt.
(2) Weiterhin werden gemäß den Aufgabenbereichen nach § 4 (2) Anwenderkreise gebildet, die sich nach Bedarf treffen. Die Termine der Anwenderkreise werden allen Teilnehmern an diesem Vertrag gemäß den nach § 4 (2) übernommenen Aufgabenbereichen mit Vorlauf von 4 Wochen bekannt gegeben. Die Anwenderkreise haben folgende Aufgaben:
   - Ermittlung von grundsätzlichem/n Änderungsbedarf/-wünschen,
   - Ermittlung von Bedarf an neuen Funktionen bzw. ggf. Abschaffung von Funktionen,
   - Erörterung/Diskussion zu ggf. vorliegenden Einzelfallproblemen,
   - Fachlicher Austausch der Anwender untereinander sowie
   - Weitergabe aller relevanten Themen, Fragestellungen etc. an den ET-Beirat des RMV.
(3) Die Informationsveranstaltung sowie die Anwenderkreise werden vom RMV organisiert und moderiert. Das Ergebnis der jeweiligen Veranstaltung ist schriftlich zu fixieren und den Teilnehmern zur Verfügung zu stellen.
(4) Der Anwenderkreis hat keine Beschlussrechte.

§ 9 Betriebskosten vHGS

Die Teilnahme am vHGS ist für die Teilnehmer kostenfrei.

§ 10 Datenschutz

(1) Soweit der RMV im Rahmen seiner Leistungserbringung für die Teilnehmer personenbezogene Daten verarbeitet ist er als Auftragnehmer (=Auftragsverarbeiter gemäß DSGVO) des Teilnehmers (=Verantwortlicher gemäß DSGVO) tätig. Die Rechte und Pflichten dieser Auftragsverarbeitung sind in Anlage 2 geregelt. Diese gilt entsprechend auch im Aufgabenbereich Vertrieb JobTicket ohne Service durch Dritte.
(2) Soweit dem Teilnehmer der Aufgabenbereich Online vHGS (inkl. Service durch Dritte) zugeordnet ist (§ 4 (2)) oder zu einem späteren Zeitpunkt zugeordnet wird, ist er zugleich Auftragnehmer für die anderen Teilnehmer mit dem Aufgabenbereich Online vHGS (inkl. Service durch Dritte) und Auftraggeber einer solchen Datenauftragsverarbeitung im Verhältnis zu diesen. Die Rechte und Pflichten der Teilnehmer sind insoweit in Anlage 3 geregelt.
(3) Alle Teilnehmer, die dem Aufgabenbereich Online vHGS (inkl. Service durch Dritte) zugeordnet sind, erkennen an, dass sie mit ihrer Unterschrift unter diesen Vertrag Auftraggeber bzw. Auftragnehmer für alle Teilnehmer sind. Eine Liste der Teilnehmer befindet sich in Anlage 7.

(4) Die diesem Vertrag als Anlagen 2 und 3 beigefügten Vereinbarungen zur Auftragsverarbeitung sind integraler Bestandteil dieses Vertrages (Anlage 3 gilt nicht für den Aufgabenbereich Vertrieb JobTicket). Mit Einführung der neuen Datenschutzgrundverordnung (DS-GVO) im Mai 2018 wurden die Anlagen 2 und 3 entsprechend aktualisiert und im Rahmen eines Vertragsänderungsverfahrens gemäß § 7 von und unter den Teilnehmern für verbindlich erklärt.

§ 11 Vertraulichkeit

(1) Die Vertragspartner verpflichten sich, sämtliche vertraulichen, geschäftlichen Informationen die ihnen im Zusammenhang mit der Vertragsabwicklung bekannt werden, vertraulich zu behandeln und ausschließlich für Zwecke des Vertrages zu verwenden. Diese Beschränkung gilt nicht für Informationen, die nachweislich zum Zeitpunkt der Überlassung öffentlich oder den Vertragspartnern bereits bekannt waren oder nach Überlassung an die Vertragspartner veröffentlicht werden, ohne dass ein Vertragspartner dies zu vertreten hätte. Die Vertragspartner stehen dafür ein, dass die Bestimmungen dieser Vertraulichkeitsklausel auch von ihren Angestellten, Erfüllungsgehilfen und Beratern beachtet werden.
(2) Die Vertragspartner unterrichten sich unverzüglich, wenn sie von einem Gericht, einer Behörde oder einem Dritten aufgefordert werden, solche vertraulichen Informationen mitzuteilen. Die Vertraulichkeitsverpflichtung gilt nicht, wenn ein Vertragspartner kraft Gesetzes oder aufgrund einer gerichtlichen oder behördlichen Verfügung vertrauliche Informationen offen legen muss, oder der andere Vertragspartner sich ausdrücklich mit einer Offenlegung einverstanden erklärt.
(3) Vertrauliche Informationen sind alle Informationen eines Vertragspartners, die entsprechend gekennzeichnet sind oder deren Vertraulichkeit sich aus der Natur der Sache oder den Umständen ergibt, unabhängig davon, ob diese verkörpert sind oder nicht.
(4) Die vorstehenden Pflichten gelten auch nach Kündigung oder Ablauf dieses Vertrages drei Jahre lang fort.

§ 12 Haftung

(1) Die Vertragspartner haften untereinander für Vorsatz und grobe Fahrlässigkeit in vollem Umfang.
(2) Im Falle einfach fahrlässigen Handelns haften die Vertragspartner ausschließlich für
- Personenschäden,
- Schäden, für die die Vertragspartner aufgrund zwingender gesetzlicher Vorschriften (z. B. nach dem Produkthaftungsgesetz) einzustehen haben sowie
- Schäden wegen der Verletzung von wesentlichen Pflichten, die die Erreichung des Zwecks des Vertrages gefährden bzw. deren Erfüllung die ordnungsgemäße Durchführung des Vertrages erst ermöglichen und auf die der andere Vertragspartner regelmäßig vertrauen darf (Kardinalpflichten).

(3) Im Falle der Verletzung von Kardinalpflichten ist die Haftung für einfach fahrlässiges Handeln auf vertragstypische und bei Abschluss des jeweiligen Vertrages vorhersehbare Schäden begrenzt.

§ 13 Aufnahme neuer Teilnehmer

Sollten besondere Umstände eintreten, die die Aufnahme eines neuen Teilnehmers erfordern, kann der RMV weitere Teilnehmer zulassen. Besondere Umstände sind insbesondere dann gegeben, wenn durch

- Ausschreibung,
- Insolvenz,
- Kommerzielle Verkehre

eine Neuaufnahme von Teilnehmern erforderlich ist.
Bei Neuaufnahme eines Teilnehmers informiert der RMV kurzfristig alle Teilnehmer über den jeweiligen Neuzugang.

§ 14 In-Kraft-Treten, Laufzeit, Kündigung

(1) Der Vertrag tritt mit Unterzeichnung in Kraft sofern der Vertragspartner bereits den Teilnahmevertrag zum (((eTicket-Deutschland (vgl. § 2 (2)) abgeschlossen hat. Wird der Teilnahmevertrag zum (((eTicket-Deutschland zeitlich später unterzeichnet, so tritt dieser Vertrag zeitgleich mit dem Vertrag zum (((eTicket-Deutschland in Kraft.

(2) Der Vertrag hat eine unbestimmte Laufzeit. Der Vertrag kann frühestens nach Ablauf von zwei Jahren seit der Aufnahme des Betriebes mit einer Kündigungsfrist von einem Jahr zum Ende eines jeden Kalenderjahres schriftlich gekündigt werden.

(3) Der Vertrag kann ferner von beiden Vertragsparteien gekündigt werden, wenn ein Teilnehmer nicht mehr im RMV-Tarifanwendungsgebiet tätig ist und keine Aufgaben gemäß § 4 (2) wahrnimmt sowie mit der Beendigung der Teilnahme am (((eTicket-Deutschland (vgl. § 2 (2)). Der Teilnehmer hat dies dem RMV unverzüglich mitzuteilen.
Die Kündigung nach Satz 1 hat schriftlich mit einer Frist von drei Monaten zum Jahresende zu erfolgen. Beide Parteien bemühen sich, soweit dies möglich ist, vor der Kündigung des Vertrages einen Kompromiss zu suchen.

(4) Das Recht auf außerordentliche Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn Umstände eintreten, die geeignet sind, erhebliche Schäden bei anderen Teilnehmern hervorzurufen oder die Systemintegrität wesentlich zu beeinflussen.
Darüber hinaus besteht ein Recht auf außerordentliche Kündigung nach § 7 (4).

(5) Der Teilnehmer kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des RMV gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages und seiner Anlagen vorliegt, der RMV eine Weisung des Teilnehmers nicht ausführen kann oder will oder der RMV Kontrollrechte des Teilnehmers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag und seinen Anlagen vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen Verstoß dar.

(6) Bei Kündigung regelt sich die Rückgabe der personenbezogenen Daten nach der Vereinbarung zum Datenschutz und zur Datensicherung in Auftragsverhältnissen nach Art. 28 DSGVO (vgl. Anlage 2 und 3).

§ 15 Schlussbestimmungen

(1) Sollten in diesem Vertrag einzelne Bestimmungen rechtsunwirksam sein oder werden, so sind sich die Vertragspartner darüber einig, dass dadurch die Gültigkeit der übrigen Bestimmungen nicht beeinträchtigt werden soll. Die unwirksame Bestimmung ist durch eine rechtswirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Dasselbe gilt, wenn bei Durchführung dieses Vertrages eine ergänzungsbedürftige Regelungslücke offenbar wird.

(2) Änderungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung des Schriftformerfordernisses.
(3) Ausschließlicher Gerichtsstand für alle Streitigkeiten, die aus diesem Vertrag resultieren, ist Frankfurt am Main.

Hofheim, den | Ort | Datum
Rhein-Main-Verkehrsverbund GmbH | Teilnehmer

_____ _____

Prof. Knut Ringat, Geschäftsführer
und Sprecher der Geschäftsführung

_____ _____

Dr. André Kavai, Geschäftsführer

RHEIN-MAIN-VERKEHRSVERBUND

Regelwerk vHGS

Regelwerk vHGS eTicket RheinMain

Anlage 1 zum vHGS-Vertrag

Thema:	Regelwerk vHGS
Dateiname:	Anlage1_Regelwerk
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	1.2
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Version als Anlage zum vHGS-Vertrag V1.0
1.1	rms	04.10.2018	Aufgabenbereich „Vertrieb von JobTickets ohne Service durch Dritte“
1.2	RMV/VGF	20.02.2019	Aufgabenbereich „Vertrieb JobTicket ohne Service durch Dritte“

Inhaltsverzeichnis

1 Einleitung

Zur Abwicklung des elektronischen Fahrgeldmanagements im RMV (eTicket Rhein-Main) nutzen die Teilnehmer (im Folgenden auch Mandanten genannt) gemeinsam das verbundweite Hintergrundsystem (vHGS). Je nach Tätigkeit im Verbund übernimmt jeder Mandant einen oder mehrere Aufgabenbereiche (vgl. § 4 vHGS-Vertrag), zu denen die in Kapitel 4 beschriebenen Aufgaben und Leistungen gehören.

2 Support

Unabhängig vom Aufgabenbereich, stehen den Mandanten folgende Supportmöglichkeiten zur Verfügung:

2.1 Fehler oder Betriebsstörungen

Bei Fehlern oder Betriebsstörungen, die bei der Nutzung des vHGS auftreten, steht die übergeordnete technische Betriebsführung (ütB) an 7 Tagen rund um die Uhr (24/7) zur Verfügung. Auf Meldungen, die per Telefon oder E-Mail erfolgen können, wird ein Mitarbeiter der ütB spätestens nach 15 Minuten reagieren. Dies gilt sowohl für die Bürozeiten Montag bis Freitag von jeweils 9:00 bis 17:00 Uhr als auch für den außerhalb der Bürozeiten organisierten Bereitschaftsdienst.

2.2 Optimierung, Weiterentwicklung oder nicht zeitkritische Probleme

Wenn Bedarf an Optimierung oder Weiterentwicklung des vHGS besteht, oder nicht zeitkritische Probleme auftreten, ist dies der übergeordneten fachlichen Betriebsführung (üfB) per Telefon oder E-Mail zu melden. Die üfB steht von Montag bis Freitag von jeweils 9:00 bis 17:00 Uhr zur Verfügung. Die gemeldeten Änderungswünsche werden von der üfB gesammelt und mit dem Mandanten, der den Bedarf angemeldet hat, abgestimmt. Sollten von dem Änderungswunsch mehrere Mandanten betroffen sein, erfolgt die Abstimmung im entsprechenden Anwenderkreis (vgl. § 8 vHGS-Vertrag).

3 Ansprechpartner

Um die Kommunikation sicherzustellen, ist von allen Mandanten, dem RMV, der ütB und der üfB mindestens ein Ansprechpartner mit E-Mailadresse und optional einer Telefonnummer zu benennen.

4 Regeln

4.1 Aufgabenbereich Online vHGS (inkl. Service durch Dritte)

4.1.1 Vertrieb und Service beim Kundenvertragspartner

Die Mandanten, die kein separates eigenes KA-fähiges Abo-/Vertriebssystem einsetzen, führen Verkaufs- und Serviceprozesse für Kunden, bei denen sie selber Vertragspartner sind (im Folgenden „eigene Kunden“ genannt), gemäß den jeweils gültigen Gemeinsamen Beförderungsbedingungen und Tarifbestimmungen (GBB) sowie den Besonderen Bedingungen über die Webanwendung des vHGS aus.

Im Rahmen der Einführung des eTicket RheinMain können eigene Kunden zukünftig bestimmte Serviceleistungen auch online über „meinRMV“ durchführen.
Der dadurch generierte Handlungsbedarf beim Mandanten wird im Aufgabenmanagement des vHGS zur Bearbeitung bereitgestellt.

Die Beschaffung der notwendigen Nutzermedien (Chipkarten) erfolgt über einen Rahmenvertrag mit der Firma Cardag Deutschland GmbH. Mit der Firma Cardag sind zwei Bestelltermine pro Jahr – der 15. Januar und der 15. Juni – verbindlich vereinbart.

Die Mandanten melden ihren Bedarf an Nutzermedien über das vHGS:

- Für den Bestelltermin am 15. Januar bis zum 01.Januar
- Für den Bestelltermin am 15. Juni bis zum 01. Juni

Folgende Serviceleistungen sind vereinbart:

Die Serviceleistungen lassen sich in zwei Kategorien unterteilen. Zum Einen in die Leistungen, die nach Eingabe des Kunden in „meinRMV“ und Übergabe in das vHGS automatisiert ablaufen (Online - Kategorie A) und zum Anderen in die Leistungen, die einen Handlungsbedarf des Mandanten auslösen (Online - Kategorie B).

Serviceleistungen Online - Kategorie A

- Vorübergehende Sperrung eines Nutzermediums
- Entsperrung eines Nutzermediums nach Wiederauffinden
- Anforderung einer Ersatzausstellung eines Nutzermediums
- Änderung der räumlichen Gültigkeit (bar)
- Änderung zu einer anderen Fahrkartenart (bar)
- Datenschutzauskunft
- Erneute Erzeugung von bei der Ausgabe des Nutzermediums erzeugten Begleitdokumenten
- Erneute Erzeugung von bei der Ausgabe von Berechtigungen erzeugten Begleitdokumenten
- Registrieren von Nutzermedien
- Änderung von Kundenstammdaten inklusive Änderung der Bankverbindung (Abo)

Serviceleistungen Online - Kategorie B

Dem Mandant werden über das Aufgabenmanagement des vHGS die nachgelagerten Aufgaben, die durch eigene Kunden Online über „meinRMV“ ausgelöst wurden, zur Bearbeitung bereitgestellt.

- Änderung der räumlichen Gültigkeit (Abo)
- Änderung zu einer anderen Fahrkartenart (Abo)

Gilt bei Abwicklung des Zahlungsverkehrs über die im vHGS integrierte Bezahlplattform:

Zur Abwicklung von Zahlungen stellt der RMV eine Bezahlplattform bereit. Der Betrieb der Bezahlplattform erfolgt durch den RMV oder einen von ihm beauftragten Dritten. Um einen reibungslosen Abrechnungsprozess zu gewährleisten ist der Teilnehmer verpflichtet die folgenden Leistungen zu erfüllen:

- Die zur Abrechnung erforderlichen Girokonten sind bei einer Bank in Deutschland zu unterhalten. Die entsprechenden Kontodaten sind an den RMV oder den von ihm benannten Dritten (=Betreiber der Bezahlplattform) weiterzuleiten. Der Teilnehmer hat seine Bank darauf hinzuweisen, dass ein zu benennender Dritter und seine Subunternehmer in seinem Auftrag Daten zur Abrechnung mit in den Bankgiroverkehr eingeben (offene Stellvertretung). Der Teilnehmer erteilt seiner Bank die Erlaubnis, dass ein zu benennender Dritter und dessen Subunternehmer in seinem Auftrag über den in die Abwicklung des Bezahlverfahrens eingeschalteten Partner Zahlungsinformationen aus dem Konto auslesen darf.
- Es ist ein Vertrag über die Bereitstellung einer technischen Schnittstelle zum elektronischen Datentransfer und weitere Leistungen mit einem Partner abzuschließen. Es ist zu regeln, dass der RMV oder ein von ihm beauftragter Dritter im Auftrag Abrechnungsdaten über diese Schnittstelle übermittelt, damit diese dann über die verschiedenen zu beteiligenden Institute die Belastung der Endkundenkonten und die Gutschrift auf dem Konto des jeweiligen Teilnehmers automatisiert anstoßen kann.
- Der Teilnehmer lässt sich von seinem Endkunden sofern dieser per elektronischen Lastschriftverkehr bezahlen möchte, eine entsprechende Einzugsermächtigung erteilen.

Gilt bei Akzeptanz von Kreditkarten:

- Der Teilnehmer ist verpflichtet, einen Kreditkartenakzeptanzvertrag über die Abwicklung von Forderungen aus der Akzeptanz von Kreditkarten (VISA oder Mastercard) mit einem Partner abzuschließen und die relevanten Vertragsdaten an den RMV oder den von ihm benannten Dritten weiterzugeben. Der Teilnehmer hat seinen Partner darauf hinzuweisen, dass der RMV oder der von ihm benannte Dritte und dessen Subunternehmer in seinem Auftrag Daten zur Abrechnung mit den Endkunden in das System des Partners eingibt (offene Stellvertretung).

- Weiterhin ist der Teilnehmer verpflichtet, sofern er Abo-Abbuchungen über ein Kreditkartenkonto anbietet, sich von seinen Endkunden eine unwiderrufliche Weisung an dessen Kreditinstitut geben zu lassen, dass der geschuldete Betrag an den Teilnehmer ausgezahlt werden soll.

4.1.2 Vertrieb und Service für Fremdkunden (Service durch Dritte)

Mit dem Ziel der Steigerung der Qualität und Kundenorientierung können im Rahmen des Services rund um das eTicket RheinMain an personalbedienten Verkaufsstellen Leistungen für dritte Vertriebspartner, die ebenfalls den Aufgabenbereich Online vHGS ausfüllen, durchgeführt werden. Ausgenommen davon sind die lokal subventionierten Tarifprodukte.

Die Serviceleistungen lassen sich in zwei Kategorien unterteilen. Zum einen in die Leistungen, die abschließend über das vHGS abgewickelt werden können (Service durch Dritte - Kategorie A), und zum anderen in die Leistungen, die neben der Eingabe im vHGS eine Weiterleitung von vom Kunden quittierten Dokumenten an den vertragsführenden KVP erfordern (Service durch Dritte - Kategorie B).

Zugriff auf Fremdkundendaten für Serviceleistungen durch Dritte

Für die Durchführung der Serviceleistungen bearbeitet der Dritte die personenbezogenen Daten des Fremdkunden im Auftrag des vertragsführenden KVP. Die Erlaubnis erhält der Dritte im Einzelfall jeweils dadurch, dass

a) der Fremdkunde das Nutzermedium zur Nutzung für die Authentifizierung vorlegt oder

b) bei fehlendem Nutzermedium sich durch Angabe personenbezogener Daten unter Vorlage eines geeigneten Nachweises authentifiziert.

Mit dem Zugriff auf die personenbezogenen Datenbereiche des Fremdkunden, bestätigt der Dritte das Vorliegen der Erlaubnis. Hierfür ist jedem Zugriff auf Fremdkundendaten eine Meldung des vHGS vorgeschaltet, die bestätigt werden muss, was im vHGS protokolliert wird. Ein Zugriff auf Daten des AG unter Umgehung dieser Funktion ist untersagt. Der vertragsführende KVP kann die von Dritten aufgenommenen Serviceleistungen und durchgeführten Datenzugriffe monatlich in einem Report abrufen. In einem zweiten Report werden monatlich die für andere KVP durchgeführten Serviceleistungen dokumentiert.

Serviceleistungen durch Dritte - Kategorie A

Bei Serviceleistungen der Kategorie A ist eine Eingabe in das vHGS erforderlich.

A1. Registrieren von Nutzermedien (nur a)
Nicht registrierte Nutzermedien sind auf Wunsch des Kunden nachträglich im vHGS zu registrieren, d.h. die Kundenstammdaten sind entsprechend aufzunehmen und im vHGS einzugeben.

A2. Änderung von Kundenstammdaten (nur a)
Die Kundenstammdaten sind auf Wunsch des Kunden zu ändern und/oder zu ergänzen. Davon ausgenommen ist die Änderung einer Bankverbindung.

A3 Sperrung der Applikation bei Verlust eines registrierten Nutzermediums
Auf Wunsch des Kunden ist bei Verlust/Diebstahl eines registrierten Nutzermediums die Applikation zu sperren. Die durch den Mitarbeiter eines Dritten erzeugte Sperranforderung, wird dem KVP über das Aufgabenmanagement des vHGS zur Prüfung vorgelegt und muss von diesem freigegeben werden.

A4 Ersatzausstellung eines Nutzermediums
Auf Wunsch des Kunden ist bei Verlust/Diebstahl/Defekt eines Nutzermediums ein Ersatz-Nutzermedium auszugeben. Das gilt sowohl für Nutzermedien mit übertragbarer als auch persönlicher Fahrberechtigung, ggf. in Form eines vorläufigen Nutzermediums. Ein Ersatz kann für alle registrierten Nutzermedien erfolgen. Ein Ersatz für anonyme Nutzermedien kann nur unter Vorlage der beim Erwerb ausgehändigten Original-Quittung erfolgen.

A5 Kündigung der ÖPV-Applikation (nur a)
Der Kunde kann seine ÖPV-Applikation kündigen, sofern keine gültige Fahrberechtigung mehr auf der Applikation vorhanden ist und er das Nutzermedium gleichzeitig zurückgibt.
Bei Kündigung erfolgt eine Löschung der ÖPV-Applikation inkl. der dazugehörigen Kundendaten. Das Nutzermedium ist einzuziehen.

A6 Annahme von gefundenen Nutzermedien
Das Nutzermedium ist entgegenzunehmen. Im Falle eines registrierten Nutzermediums, für das noch kein Ersatz ausgestellt wurde, ist mit dem Inhaber des Nutzermediums Kontakt aufzunehmen und mit ihm abzustimmen, wie mit dem Nutzermedium weiter verfahren werden soll. Im Falle eines anonymen Nutzermediums ist die Applikation zu sperren und das Nutzermedium einzuziehen.

A7 Datenschutzauskunft (nur a)
Jeder Kunde erhält auf Wunsch eine Auskunft über die im eTicket RheinMain mit seinen Stammdaten oder seinem Nutzermedium verknüpften Informationen. Diese sind dem Kunden auszudrucken und auszuhändigen.

Infolge der beschriebenen Serviceprozesse eingezogene Nutzermedien sind zu sammeln und halbjährlich an die „übergeordnete fachliche Betriebsführung“ des vHGS zu versenden.

Serviceleistungen durch Dritte - Kategorie B

Bei Serviceleistungen der Kategorie B sind nach der Eingabe ins vHGS **immer** zusätzlich die entsprechenden Eingaben, Änderungen, Aktualisierungen etc. auszudrucken und vom Kunden zu unterschreiben. Der Kunde bestätigt damit, die Korrektheit und Vollständigkeit der Eingaben. Die Belege sind bis zum 11. des Vormonats an den vertragsführenden KVP per Fax, gemäß der im vHGS hinterlegten Kontaktliste zu übersenden.

Die nachgelagerten Aufgaben werden dem vertragsführenden KVP im Aufgabenmanagement des vHGS bereitgestellt.

Der vertragsführende KVP kann - wie bei Kategorie A - über das vHGS einen Report über Eingaben, Änderungen und Aktualisierungen, die von Dritten durchgeführt wurden, abrufen.

B1 Änderung der räumlichen Gültigkeit (Abo)
Die Änderung der räumlichen Gültigkeit einer Fahrberechtigung im Abo auf einem registrierten Nutzermedium ist auf Wunsch des Kunden im System zur weiteren Verarbeitung zu erfassen.
Der durch Dritte aufgenommene Änderungswunsch wird dem zuständigen KVP über das Aufgabenmanagement des vHGS angezeigt. Der zuständige KVP hat den Änderungswunsch zu prüfen und bei positivem Ergebnis bis zum 25. des Vormonats über das Aktionsmanagement dem Kunden als Aktion bereit zu stellen. Der Kunde ist über das Ergebnis der Prüfung vor dem 25. des Vormonats schriftlich zu informieren.

B2 Änderung zu einer anderen Fahrkartenart (Abo)
Die Änderung zu einer anderen Fahrkartenart ist auf Wunsch des Kunden im System zur weiteren Verarbeitung zu erfassen. Ausgenommen ist die Änderung von einer übertragbaren zu einer persönlichen Fahrkartenart. Der durch Dritte aufgenommene Änderungswunsch wird dem zuständigen KVP über das Aufgabenmanagement des vHGS angezeigt. Der zuständige KVP hat den Änderungswunsch zu prüfen und bei positivem Ergebnis bis zum 25. des Vormonats über das Aktionsmanagement dem Kunden als Aktion bereit zu stellen. Der Kunde ist über das Ergebnis der Prüfung vor dem 25. des Vormonats schriftlich zu informieren.

4.2 Aufgabenbereich Offline vHGS

Die Ausgabe von Nutzermedien und Verkäufe von Fahrberechtigungen sind prinzipiell auch offline zum vHGS möglich. Diese Option kann in folgenden Fällen genutzt werden, wobei auch eine Kombination möglich ist:

1. Verkehrsunternehmen verfügen über ein eigenes KA-fähiges Vertriebs- und Abosystem für den Verkauf von Jahresabos und ggf. auch weiterer Fahrkartenarten oder
2. Verkehrsunternehmen geben elektronische Fahrberechtigungen über Busdrucker und stationäre Fahrausweisautomaten aus.

Im **ersten Fall** ist geplant, diese Hintergrundsysteme voraussichtlich im Sommer 2012 über eine bidirektionale Schnittstelle mit dem vHGS zu verbinden, so dass diese Unternehmen als Teilnehmer der RMV KVP-Agentur in das verbundweite Servicekonzept („Service durch Dritte“) eingebunden werden können. Die Regeln für den entsprechenden Aufgabenbereich sind in Übereinstimmung mit dem noch zu erarbeitenden Konzept zur bidirektionalen Schnittstelle zu definieren. Dies gilt auch für die Aufteilung der dadurch resultierenden Kosten zwischen den Beteiligten.

Für die Zeit vom Systemstart des eTicket RheinMain (Dezember 2011) bis zur Herstellung der Betriebsbereitschaft der bidirektionalen Schnittstelle, müssen die Systeme über die Schnittstelle des vHGS für einen so genannten externen Mandant (siehe Anlage 6 zum vHGS-Vertrag: „Konzept Externer Mandant“) mit dem vHGS verbunden werden.

Der RMV stellt im vHGS, die Verkehrsunternehmen in ihren Systemen die entsprechende Schnittstelle bereit.

Im **zweiten Fall** sind folgende Voraussetzungen zu erfüllen:

- Als Offline-Verkaufsgeräte sind KA-konforme Geräte mit einem SAM einzusetzen. Für die an das vHGS gemeldeten Applikations- und Berechtigungsausgaben verwenden die Offline-Verkaufsgeräte die gemeinsamen KVP-Schlüssel des eTicket RheinMain.
- Das Verkehrsunternehmen betreibt ein Terminalmanagementsystem (vgl. PH06-02), das die Daten der Verkaufsgeräte sammelt und an das vHGS täglich weiterleiten kann.
- Das Terminalmanagementsystem bezieht täglich zu einer abgestimmten Zeit Sperr- und Aktionslisten vom vHGS (vgl. Kap. 4.4) und aktualisiert die Verkaufsgeräte ebenfalls täglich vor der ersten Nutzung mit den Sperr- und Aktionslisten.
- Das Terminalmanagementsystem bezieht Zertifikate und Kryptogramme vom vHGS und verteilt diese an die Verkaufsgeräte. Der Mandant ist angehalten mittelfristig Verkaufsgeräte im Einsatz zu haben, die in der Lage sind, die Zertifikate und Kryptogramme KA-konform in die SAMs zu laden.

4.3 Aufgabenbereich TicketShop

Bestellungen von Kunden im RMV-TicketShop werden entsprechend den Regelungen des § 6 des vHGS-Vertrags vor der Übergabe an das vHGS einem Kundenvertragspartner (KVP) zugeordnet. Diese Bestellungen müssen gemäß den jeweils gültigen Gemeinsamen Beförderungsbedingungen und Tarifbestimmungen (GBB) sowie den Besonderen Bedingungen gegenüber dem Kunden im vHGS mit Hilfe des Aufgabenmanagements bearbeitet werden. Die Bearbeitung einer durch den Kunden eingegebenen Bestellung erfolgt dabei nach denselben Regeln, wie die Bearbeitung der durch den Mitarbeiter in der pVks erfassten Bestellung. Die möglichen Aufgaben entsprechen daher denen in Kapitel 4.1.1. mit Ausnahme solcher Servicefälle, die einen Wechsel der beim initialen Kauf genutzten Zahlart und des dazugehörigen Vertriebskanals bedingen würden.
Da Kundenbelege nicht persönlich übergeben werden können, sind diese per Post oder E-Mail zuzustellen.

4.4 Aufgabenbereich Kontrolle

Teilnehmer mit dem Aufgabenbereich Kontrolle gewährleisten die Erfüllung folgender Leistungen im Rahmen des vHGS:

1. Das unternehmenseigene Terminalmanagementsystem ist mit einer Schnittstelle[1] zum vHGS auszustatten, um den Austausch von Sperr- und Aktionsliste, sowie von Sperr- und Transaktionsnachweisen sicherzustellen.
2. Die Sperrlisten, die im vHGS um 00:30 Uhr bereitgestellt werden, sind täglich auf allen im Unternehmen eingesetzten Kontrollgeräten[2] zu aktualisieren.
3. Sofern Kontrollgeräte für die Ausgabe von Aktionen im Aktionsmanagement vorgesehen sind, muss die Aktionsliste, die im vHGS um 00:30 Uhr bereitgestellt wird, täglich auf den entsprechenden Kontrollgeräten aktualisiert werden.
4. Die aufgrund der Kontrolltätigkeit entstehenden Sperrnachweise sowie ggf. Transaktionsnachweise aus dem Aktionsmanagement, sind mindestens einmal täglich an das vHGS zu übertragen. Nachweise, die bis 22:00 Uhr übertragen werden, werden im Rahmen der Erstellung der Sperr- und Aktionslisten des Folgetages berücksichtigt.
5. Die aufgrund der Kontrolltätigkeit entstehenden Kontrollnachweise sind mindestens alle zwei Wochen an das vHGS zu übertragen. Bis zur Genehmigung des Verfahrens zur Verarbeitung personenbezogener Daten für Zwecke der Betrugsbekämpfung im Rahmen des PH 04 ist die Lieferung der Kontrollnachweise keine Pflicht.

[1] Die Schnittstelle zum vHGS ist im PH06-02_Terminalmanagementsysteme beschrieben.
[2] Kontrollgeräte: Busdrucker, Einstiegskontrollterminal, mobiles Kontrollgerät

4.5 Aufgabenbereich Vertrieb JobTicket ohne Service durch Dritte

Teilnehmer mit dem Aufgabenbereich Vertrieb JobTicket ohne Service durch Dritte sind für die Ausgabe und Verwaltung von JobTickets zuständig bzw. unmittelbar gegenüber dem JobTicketunternehmen berechtigte Verkehrsunternehmen. Dabei nutzen Teilnehmer das vHGS alleine für die Verwaltung und Ausgabe von JobTickets an die Mitarbeiter eines JobTicketunternehmens, gegenüber denen Teilnehmer bezüglich der einzelnen an die Nutzer ausgegebenen Fahrkarten in der Rolle als Kundenvertragspartner (KVP) auftreten. Sofern weitere Produkte des eTicket RheinMain durch die Teilnehmer verkauft und verwaltet werden, geschieht dies außerhalb des vHGS. Im vHGS besteht grundsätzlich kein Zugriff seitens der Teilnehmer auf die Daten der Mitarbeiter des JobTicketunternehmens. Dies gilt sowohl für die Ausgabe als auch für die Verwaltung der JobTickets durch die Teilnehmer. Lediglich die Namen und Email-Adressen der vHGS-Administratoren auf Seiten der JobTicketunternehmen sind den Teilnehmern bekannt, da diese die Administratoren anlegen müssen (s. u., Punkt 3).

Die Teilnehmer gewährleisten die Erfüllung folgender Leistungen:

1. JobTicketunternehmen, die direkt mit den JobTicketprozessen im vHGS starten oder vom eAD auf das vHGS migrieren, werden durch das betreuende VU fachlich, organisatorisch und schulungstechnisch unterstützt.
2. Für jedes JobTicketunternehmen muss der Teilnehmer im vHGS eine Unternehmenseinheit anlegen, die insoweit die maßgebliche Vertriebsstelle repräsentiert, über die die vom JobTicketunternehmen mit der Ausgabe und Verwaltung des JobTickets betrauten Mitarbeiter ihre Aufgaben wahrnehmen können.
3. Um den zuvor genannten Mitarbeitern im JobTicketunternehmen den erforderlichen Zugang zum vHGS zu verschaffen, legt das betreuende Verkehrsunternehmen ein Benutzerkonto für den Administrator im JobTicketunternehmen an. Alle weiteren Benutzerkonten kann dieser Administrator selbst anlegen und verwalten. Diese selbst angelegten Benutzerkonten haben allerdings keine Administratorrechte.
4. Dem JobTicketunternehmen ist ein Bestand an Chipkartenrohlingen und ggfs. Wertmarkenbögen zur Verfügung zu stellen. Diese (Chipkartenrohlinge) werden benötigt, um per Schreib-/Leseeinheit JobTickets für neue Mitarbeiter und Ersatzchipkarten ausstellen zu können. Wenn der Erstversand nicht über den Massenpersonalisierer erfolgt (<50 JobTickets), werden die Chipkartenrohlinge bereits bei der Erstausgabe benötigt. Weiterhin kann das JobTicketunternehmen auch laufend Rohlinge beim VU nachbestellen.
5. Der Teilnehmer (Verkehrsunternehmen) stellt seinen JobTicketunternehmen eine monatliche Rechnung auf Basis der dazu nötigen Meldung der Berechtigten und übernimmt im Folgenden das Forderungsmanagement.

RHEIN-MAIN-VERKEHRSVERBUND

Vereinbarung zur Auftragsverarbeitung
RMV-Teilnehmer

Vereinbarung
zum Datenschutz und zur Datensicherheit in
Auftragsverhältnissen nach Art. 28 DSGVO

Anlage 2 zum vHGS-Vertrag

zwischen

allen Mandanten im vHGS mit dem Aufgabenbereich Online vHGS
(vgl. Anlage 7 zum vHGS-Vertrag)

- **nachstehend auch gemeinsam „Auftraggeber (AG)“ genannt –**

und
der

Rhein-Main-Verkehrsverbund GmbH (RMV)
Alte Bleiche
Hofheim am Taunus

- nachstehend auch „Auftragnehmer (AN)“ genannt -

Thema:	Vereinbarung Auftragsdatenverarbeitung RMV-Teilnehmer
Dateiname:	Anlage2_Vereinbarung gem Art. 28 DSGVO RMV_Teilnehmer
Erstellt am:	08.12.2011
Zuletzt geändert am:	06.06.2019
Version:	1.2
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Version als Anlage zum vHGS-Vertrag V1.0
1.1	RMV	20.02.2019	Anpassungen an die DSGVO
1.2	RMV	06.06.2019	Anpassung § 5 lt. 15 – Datenschutzverantwortlicher RMV

§ 1 Gegenstand der Vereinbarung

(1) Der AN verarbeitet auf Grundlage dieses Vertrages personenbezogene Daten im Sinne von Art. 4 Nr. 2 DSGVO (Datenschutzgrundverordnung) gemäß Art. 28 DSGVO im Auftrag des AG im Rahmen der technischen und fachlichen Betriebsführung des eTicket RheinMain in einem dafür von der Firma Cubic Transportation Systems (Deutschland) GmbH für den RMV entwickelten webbasierten verbundweiten Hintergrundsystem (vHGS). (Weitere Details zu den Leistungen des AN sind im vHGS-Vertrag inkl. seiner Anlagen geregelt.)

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Der AN verarbeitet personenbezogene Daten des AG ausschließlich in dessen Auftrag.

(4) Die Dauer dieser Vereinbarung richtet sich nach der des Vertrages über die Nutzung, Teilnahme und Zusammenarbeit am verbundweiten mandantenfähigen Hintergrundsystem (vHGS) des eTicket RheinMain.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen, Empfänger von personenbezogenen Daten

Der AN betreibt unter der Bezeichnung vHGS für den AG (=Teilnehmer bzw. Mandant) sowie weitere Teilnehmer/Mandanten eine Datenbank zur Verwaltung von Kundendaten zum Zweck des Vertriebs elektronischer Fahrscheine auf Chipkarte und deren Kontrolle sowie Papierfahrscheinen im Rhein-Main-Verkehrsverbund. Der AN übernimmt für den AG den fachlichen und technischen Betrieb des vHGS.

Betroffene Personen und Art der personenbezogenen Daten:

Kategorien betroffener Personen	**Art der personenbezogenen Daten**
Stammdaten der Kunden	<u>Personenstammdaten:</u> Name, Vorname, Geschlecht, Titel, Geburtsdatum, Adresse (Straße, Hausnummer, Postleitzahl, Ort), E-Mail-Adresse, Telefon <u>Vertragsstammdaten:</u> Bankverbindung (IBAN, BIC, Name des Bankinstituts), Kundennummer, Vertragsnummer, Chipkartennummer, zugeordnete Rolle (Besteller, Bezahler, Benutzer der Fahrkarte) <u>Sonstige Daten:</u> Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke, bspw. Nutzung des eTickets, Bonusprogramm RMVsmiles
Nutzungsdaten der Kunden	<u>Verkaufs-/Fahrkartendaten:</u>

	Berechtigungs-ID, Tarifprodukt (Fahrkartenart), Vertragspartner (leistungserbringendes Verkehrsunternehmen), Verkaufsdatum, Verkaufsuhrzeit, Start und Ziel Tarifgebiet, Beginn und Ende Gültigkeit, Preis Kontrolldaten(satz): Datum, Zeit, Orts-Nummer, Chipkarten-Nr., Berechtigungs-ID Zahlungsdaten: Ergebnis der Bonitätsprüfung, Zahlungseingang Transaktionsdaten (Chipkarte): Die letzten 10 Transaktionen (Daten, die zwischen Chipkarte und Verkaufs-/Kontrollterminal ausgetauscht werden) auf der Chipkarte (Zeit, Ort und Art der Transaktion, Terminalnummer, Ticket-/Produktnummer)
Stammdaten der zugriffsberechtigten Mitarbeiter des AG	Benutzerkennung, Benutzerstammdaten gemäß Benutzerverwaltung der Anwendung, dem Benutzer zugeordnete Gerätekennung
Stammdaten der Lieferanten, Dienstleister	Adressdaten, Bankverbindungen, Vertragsdaten, Abrechnungs- und Leistungsdaten
Nutzungsdaten des AN/AG	Meldung des vHGS über Zugriff auf Fremdkundendaten (Bestätigung über das Vorliegen einer Erlaubnis des Kunden)

Es werden keine besondere Arten personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO erhoben.

Auf die nachstehenden Daten oder Datenkategorien hat der AN nicht nur Zugriff, sondern leitet diese auftragsgemäß auch an die aufgeführten Empfänger weiter:

Empfänger oder Kategorien von Empfängern	**Zweck und Art der Weiterleitung**
AN, Dienstleister/Subunternehmer	
Auskunftei für Bonitätsauskunft	Über Standardschnittstelle Bonitätsauskunft; Name, Anschrift, Geburtsdatum
Geldinstitute	Über Standardschnittstelle Zahlungsverkehr; Name, Bankverbindung, Zahlungsdaten
Inkassodienstleister	Über Standardschnittstelle Forderungsdienstleistung; Name, Anschrift, Geburtsdatum, Bankverbindung, Forderungsdaten
Am eTicket teilnehmende Unternehmen	Über Standardschnittstelle der eTicket-Anwendung; eTicket-Kennung in Verkaufs-, Kontroll- und Transaktionsdaten, Geräte-Kennung, SAM-ID in Verkaufs-, Kontroll- und Transaktionsdaten
AN/RMV	Über Standardschnittstelle der eTicket-Anwendung; Geräte-Kennung, SAM-ID in Verkaufs-, Kontroll- und Transaktionsdaten

Massenpersonalisierer	Über Standardschnittstelle Massenpersonalisierer: Personen- und Vertragsstammdaten sowie Verkaufs-/Fahrkartendaten des Kunden

Jegliche Datenverarbeitung zur Verwaltung von Kundendaten zum Zweck des Vertriebs der elektronischen Fahrkarte und deren Kontrolle erfolgt nach Maßgabe des vHGS-Vertrages.
Darüber hinaus können die in der Datenbank des vHGS gespeicherten Daten auch für die nachstehenden Verbundleistungen der Vertriebsunterstützung genutzt werden, wie

- die Betreuung von Kunden und Interessenten, u.a.
  - im Rahmen der schriftlichen Kundenkommunikation sowie
  - durch das Call Center (ausgenommen ist der Aufgabenbereich JobTicket),
- die Bewerbung von Produkten und Marketingaktionen, u.a.
  - RMV-Smiles (ausgenommen ist der Aufgabenbereich JobTicket),
    Der RMV (AN) betreibt ein online und mobil nutzbares Bonusprogramm mit der Bezeichnung „RMVsmiles – Das Bonusprogramm“ (nachfolgend: RMVsmiles). Registrierte RMV-Kunden, welche ihre Fahrkarten über den Dienst TicketShop unter meinRMV (www.rmv.de) erwerben, sammeln nach entsprechender Anmeldung für das Bonusprogramm Bonuspunkte (Smiles), mit welchen sie Rabatt-Gutscheine verschiedener Anbieter erwerben können. Während des Bestellvorgangs einer Fahrkarte im TicketShop werden dem Nutzer noch im Warenkorb die Smiles in Bezug auf den Warenwert-Betrags angezeigt. Der Warenwert-Betrag wird zusammen mit der Kunden-ID und der Information der Bonusteilnahme des Kunden an das vHGS gesendet. Nach erfolgreicher Abbuchung des Warenwert-Betrags sendet das vHGS eine entsprechende Information (Abbuchung ist erfolgt) samt Kunden-ID an den Smiles-Berechner zurück. Die Kunden-ID und erworbene Punkte werden in der Smiles-Datenbank gespeichert.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für Wahrung der Rechte der Betroffenen nach Art. 12 bis 22 DSGVO ist der jeweils Verantwortliche, abhängig von der betroffenen Datenverarbeitung, allein verantwortlich. Gleichwohl ist der AN verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind – soweit dies keine Vertragsänderung gemäß § 7 des vHGS-Vertrages erfordern würde – gemeinsam abzustimmen und schriftlich festzulegen.

(3) Der AG erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die Weisungsbefugnis des AG beschränkt sich auf die von ihm gemäß DSGVO verantworteten und in seinem Auftrag verarbeiteten Daten, Weisungen an den AN, die die Verarbeitung bzw. Löschung der auch von anderen AG verantworteter Daten betreffen, können nur von den betroffenen AG gemeinsam angewiesen werden.

(4) Der AG ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der AG kann diese Kontrolle auch durch einen Dritten durchführen lassen.

(5) Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der AG ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherungsmaßnahmen des AN vertraulich zu behandeln.

§ 4 Weisungsberechtigte des AG, Weisungsempfänger des AN

Weisungsberechtigte Personen des AG sind die jeweiligen Geschäftsführer und/oder die Mitglieder des Vorstandes und/oder die der Anlage 12 genannten Personen.

Weisungsempfänger beim AN sind neben den Geschäftsführern des AN die in Anlage 12 genannten Personen.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 5 Pflichten des Auftragnehmers

(1) Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der AG dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit a DSGVO).

(2) Der AN verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene bzw. nicht vom AG freigegebene Zwecke. Kopien oder Duplikate werden ohne Wissen des AG nicht erstellt.

(3) Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen vHGS-fremden Datenbeständen strikt getrennt werden. Für den Aufgabenbereich JobTicket sichert der AN zu, dass nur das jeweils als abrechnende Stelle eingesetzte VU/AG Einsicht in und Zugriff auf die personenbezogenen Datenbestände derjenigen Vertragspartner im JobTicket hat, für die er die Abrechnung und Betreuung wahrnimmt.

(4) Die Datenträger, die vom AG stammen bzw. für den AG genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden – automatisierten- Verwaltung. Eingang und Ausgang werden dokumentiert.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den AG, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten des AG hat der AN im notwendigen Umfang mitzuwirken und den AG soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

Insbesondere unterstützt der AN den AG bei der Ausübung des Auskunftsanspruchs von betroffenen Personen gemäß Art. 15 DSGVO durch Bereitstellung einer Funktionalität im vHGS zum Abruf seiner dort gespeicherten Daten.

(6) Der AN wird den AG unverzüglich darauf aufmerksam machen, wenn eine vom AG erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim AG nach Überprüfung bestätigt oder geändert wird.

(7) Der AN hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der AG dies mittels einer

Weisung verlangt und berechtigte Interessen des AN oder anderer AG dem nicht entgegenstehen.

(8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder in Ausübung der Betroffenenrechte nach der DSGVO an den Betroffenen selbst darf der AN nur nach vorheriger Weisung oder schriftlicher Zustimmung durch den AG erteilen.

(9) Der AN erklärt sich damit einverstanden, dass der AG – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom AG beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der AN sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(10) Die Verarbeitung von Daten außerhalb geschützter geschäftlicher Infrastruktur beim AN respektive bei dessen Subunternehmer ist nicht gestattet. Die Sicherungsmaßnahmen gem. § 8 sind zu gewährleisten.

(11) Der AN bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

(12) Der AN verpflichtet sich, bei der auftragsgemäßen Verarbeitung personenbezogener Daten des AG die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(13) Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeiten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigtenverhältnisses in geeigneter Weise zu Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der AN überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(14) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem AG abzustimmen.

(15) Beim AN ist als Beauftragter für den Datenschutz
Herr Oliver Krause
- externer Datenschutzbeauftragter -
E-Mail: datenschutzbeauftragter@rmv.de
bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.

§ 6 Mitteilungspflichten des AN bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der AN teilt dem AG unverzüglich Störungen, Verstöße des AN oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des AG nach Art. 33 und Art. 34 DSGVO. Der AN sichert zu, den AG erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den AG darf der AN nur nach vorheriger Weisung gemäß § 4 dieses Vertrages durchführen.

§ 7 Unterauftragsverhältnisse mit Subunternehmern

(1) Der AN ist nach § 3 Abs. 5 vHGS-Vertrag berechtigt zur Erfüllung seiner Leistungen Subunternehmer einzusetzen.

(2) Der AN bedient sich bei der Erbringung des fachlichen und technischen Betriebs des vHGS seiner 100%igen Tochter der rms GmbH in Frankfurt am Main. Weiterhin beauftragt der AN ein Unternehmen mit der Massenpersonalisierung der notwendigen Nutzermedien, die der AG im Rahmen des Vertriebs seinen Kunden zur Verfügung stellt.

Die rms GmbH wiederum hat den technischen Betrieb inkl. der Wartung und Pflege, das Hosting sowie den Second-Level-Support an den Hersteller der verwendeten Software, die Firmal Cubic in Hamburg, ausgelagert. Die Firma Cubic wiederum bedient sich eines externen Rechenzentrums. (vgl. auch Liste der Subunternehmer in der Anlage zum Hauptvertrag).

(3) Die Beauftragung von Subunternehmern ist dem AG schriftlich mit Name und Anschrift bekannt zu geben. Der AN versichert, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem AG auf Anfrage zur Verfügung zu stellen.

Der AN hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen AG und AN auch gegenüber Subunternehmern gelten. Insbesondere muss der AG berechtigt sein, im Bedarfsfall angemessene Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der AN hat die Einhaltung der Pflichten aus § 8 dieses Vertrages regelmäßig – mindestens einmal jährlich – zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem AG auf Verlangen zugänglich zu machen.

In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des AN und des Subunternehmers deutlich voneinander abgegrenzt sind. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach Art. 29 und Art. 32 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der AN haftet gegenüber dem AG dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

Zurzeit sind die in der dem vHGS-Vertrag nachrichtlich beigefügten „Liste mit Subunternehmern des RMV“ mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Die Liste mit Subunternehmern des RMV ist immer aktuell zu halten und dem AG zur Verfügung zu stellen. Mit deren Beauftragung erklärt sich der AG einverstanden.

§ 8 Technische und organisatorische Maßnahmen nach § 9 BDSG

(1) Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzen der AN oder die von ihm beauftragten Dritten das hierfür entwickelte webbasierte mandantenfähige verbundweite Hintergrundsystem (vHGS). Eine Beschreibung der Organisation und Datenverarbeitung sowie des Sicherheitsmanagements im vHGS befindet sich in Anlage 11.

(2) Der AN beachtet die Grundsätze der ordnungsgemäßen Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherungsmaßnahmen.

(3) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen haben die Verantwortlichen und der Auftragsverarbeiter (auch unter Berücksichtigung von UAN) geeignete technische und

organisatorische Maßnahmen (TOM) getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen u.a. Folgendes ein:

a) Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Weitere Details dazu wurden in den Datensicherungskonzepten bzw. den TOMs (technische und organisatorische Maßnahmen) der verschiedenen Beteiligten geregelt. Die dort enthaltenen Sicherheitsniveaus sind zwischen dem AN und demjenigen, um dessen Datensicherungskonzept/TOMs es sich handelt, abgestimmt und werden vom AN gewährleistet.

Die nachfolgend aufgeführten Datensicherungskonzepte/TOMs sind verbindlich und werden mit Vertragsabschluss Vertragsbestandteil.

- Anlage 10 (TOMs rms GmbH),
- Anlage 4 (TOMs Technischer Betreiber) und
- Anlage 5 (TOMs Massenpersonalisierer).

Der AN hat kein (direkten) Zugriff bzw. keine Einsicht auf personenbezogene Daten im vHGS. Jegliche diesbezügliche Leistungen sind an UAN vergeben (vgl. § 7).

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen sind zwischen AG und AN schriftlich zu vereinbaren.

(5) Soweit die beim AN getroffenen Sicherheitsmaßnahmen den Anforderungen des AG nicht genügen, benachrichtigt er den AG unverzüglich.

(6) Der AN hat bei gegebenem Anlass, mindestens aber alle zwei Jahre, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen. Das Ergebnis samt vollständigem Auditbericht ist dem AG mitzuteilen.

§ 9 Verpflichtungen des AN nach Beendigung des Auftrages, Art. 28 Abs. 3 Satz 2 lit g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der AN sämtliche in seinem Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen und/oder datenschutzgerecht zu löschen bzw. zu vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem AG mit Datumsangabe schriftlich zu bestätigen.

§ 10 Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der AG gegenüber dem Betroffenen verantwortlich, soweit es nicht zum Einsatz eines verantwortlichen VDL nach § 4 Abs. 6 des vHGS-Vertrages kommt. Soweit der AG zum Schadensersatz

gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim AN vorbehalten, wenn dieser den Schaden vorsätzlich oder fahrlässig verursacht hat. Es gelten die Regelungen des §12 vHGS-Vertrag.

§ 11 Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmern) sind von beiden Vertragsparteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

RHEIN-MAIN-VERKEHRSVERBUND

Vereinbarung zur Auftragsverarbeitung
Teilnehmer untereinander

Vereinbarung

zum Datenschutz und zur Datensicherung in

Auftragsverhältnissen nach Art. 28 DSGVO

Anlage 3 zum vHGS-Vertrag

zwischen
den Mandanten im vHGS
mit dem Aufgabenbereich Online vHGS jeweils untereinander
(wobei jeder gegenüber allen anderen sowohl
Auftraggeber als auch Auftragnehmer ist)
(vgl. Anlage 7 zum vHGS-Vertrag)

_____

-nachstehend gemeinsam „Auftraggeber (AG) und Auftragnehmer (AN)“
genannt-

Thema:	Vereinbarung Auftragsdatenverarbeitung Teilnehmer untereinander
Dateiname:	Anlage3_Vereinbarung gem Art. 28 DSGVO Teilnehmer_Teilnehmer
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	1.1
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Version als Anlage zum vHGS-Vertrag V1.0
1.1	RMV	20.02.2019	Anpassungen an die DSGVO

§ 1 Gegenstand der Vereinbarung

(1) Der AN verarbeitet auf Grundlage dieses Vertrages personenbezogene Daten im Sinne von Art. 4 Nr. 2 DSGVO (Datenschutzgrundverordnung) im Auftrag des AG im Rahmen des eTicket RheinMain in einem dafür von der Firma Cubic Transportation Systems (Deutschland) GmbH für den RMV entwickelten webbasierten verbundweiten Hintergrundsystem (vHGS). (Weitere Details zu den Leistungen des AN sind im vHGS-Vertrag inkl. seiner Anlagen geregelt.)

(2) Das vHGS unterstützt gleichzeitig identische Auftragsverarbeitung zwischen jeweils mehreren AG und AN.

(3) Die Datenverarbeitung im Auftrag beginnt mit dem Zugriff eines Mandanten des vHGS (Rolle des AN) auf die Kundendaten eines anderen Mandanten des vHGS (Rolle des AG) gemäß Regelwerk (Anlage 1 zum vHGS-Vertrag), Abschnitt 4.1.2 oder mit der entsprechend vorausgehenden Datenerhebung beim Fremdkunden für Zwecke der Authentifizierung und Autorisierung.

(4) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in einem Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 2 Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen, Empfänger von personenbezogenen Daten

Die Datenverarbeitung im vHGS erfolgt zur Ausübung des Service durch Dritte sowie der gemeinsamen Nutzung von Kundenstammdaten im Rahmen des eTicket RheinMain. Der AN übernimmt für den AG die Bearbeitung von Kundenstamm- und vertragsdaten gemäß Regelwerk (Anlage 1 zum vHGS-Vertrag) soweit sich ein Kunde des AG an den AN zur Durchführung eines Services wendet.

Betroffene Personen und Art der personenbezogenen Daten:

Kategorien betroffener Personen	**Art der personenbezogenen Daten**
Stammdaten der Kunden	<u>Personenstammdaten:</u> Name, Vorname, Geschlecht, Titel, Geburtsdatum, Adresse (Straße, Hausnummer, Postleitzahl, Ort), E-Mail-Adresse, Telefon <u>Vertragsstammdaten:</u> Bankverbindung (IBAN, BIC, Name des Bankinstituts), Kundennummer, Vertragsnummer, Chipkartennummer, zugeordnete Rolle (Besteller, Bezahler, Benutzer der Fahrkarte) <u>Sonstige Daten:</u> Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke,

	bspw. Nutzung des eTickets, Bonusprogramm RMVsmiles
Nutzungsdaten der Kunden	Verkaufs-/Fahrkartendaten: Berechtigungs-ID, Tarifprodukt (Fahrkartenart), Vertragspartner (leistungserbringendes Verkehrsunternehmen), Verkaufsdatum, Verkaufsuhrzeit, Start und Ziel Tarifgebiet, Beginn und Ende Gültigkeit, Preis Zahlungsdaten: Ergebnis der Bonitätsprüfung (als Ampel) Transaktionsdaten (Chipkarte): Die letzten 10 Transaktionen (Daten, die zwischen Chipkarte und Verkaufs-/Kontrollterminal ausgetauscht werden) auf der Chipkarte (Zeit, Ort und Art der Transaktion, Terminalnummer, Ticket-/Produktnummer)
Nutzungsdaten des AN/AG	Meldung des vHGS über Zugriff auf Fremdkundendaten (Bestätigung über das Vorliegen einer Erlaubnis des Kunden)

Es werden keine besondere Arten personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO erhoben.

Jegliche Datenverarbeitung zur Verwaltung von Kundendaten zum Zweck des Vertriebs der elektronischen Fahrkarte und deren Kontrolle erfolgt nach Maßgabe des vHGS-Vertrages.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie fürdie Wahrung der Rechte der Betroffenen nach Art. 12 bis 22 DSGVO ist allein der AG verantwortlich. Der AN ist verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den AG gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind – soweit dies keine Vertragsänderungen gemäß § 7 des vHGS-Vertrages erfordern würde – gemeinsam abzustimmen und schriftlich festzulegen.

(3) Die Weisungsbefugnis des AG beschränkt sich auf die von ihm gemäß DSGVO verantworteten und in seinem Auftrag verarbeiteten Daten, Weisungen an den AN, die die Verarbeitung bzw. Löschung der auch von anderen AG verantworteter Daten betreffen, können nur von den betroffenen AG gemeinsam angewiesen werden.

(4) Der AG ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der AG kann diese Kontrolle auch durch einen Dritten durchführen lassen.

(5) Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der AG ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherungsmaßnahmen des AN vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 4 Weisungsberechtigte des AG, Weisungsempfänger des AN

(1) Weisungsberechtigte Personen des AG sind die jeweiligen Geschäftsführer und/oder die Mitglieder des Vorstandes.

(2) Weisungsempfänger beim AN sind neben den Geschäftsführern des AN die in Anlage 12 des Teilnahmevertrages genannten Personen.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 5 Pflichten des Auftragnehmers

(1) Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der AG dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit a DSGVO.

(2) Der AN verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene bzw. nicht vom AG freigegebene Zwecke. Kopien oder Duplikate werden ohne Wissen des AG nicht erstellt.

(3) Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt vHGS-fremden werden.

(4) Die Datenträger, die vom AG stammen bzw. für den AG genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden – automatisierten- Verwaltung. Eingang und Ausgang werden dokumentiert.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den AG, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des AG hat der AN im notwendigen Umfang mitzuwirken und den AG soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

(6) Der AN wird den AG unverzüglich darauf aufmerksam machen, wenn eine vom AG erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim AG nach Überprüfung bestätigt oder geändert wird.

(7) Der AN hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der AG dies mittels einer Weisung verlangt und berechtigte Interessen des AN oder anderer AG dem nicht entgegenstehen.

(8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder in ausdrücklicher und über eine Auskunftserteilung im Rahmen üblicher Kundenbetreuung hinausgehende Ausübung der Betroffenenrechte nach der DSGVO an den Betroffenen selbst darf der AN nur nach vorheriger Weisung oder schriftlicher Zustimmung durch den AG erteilen.

(9) Der AN erklärt sich damit einverstanden, dass der AG grundsätzlich nach Terminvereinbarung berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom AG beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die

gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der AN sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(10) Die Verarbeitung von Daten außerhalb geschützter geschäftlicher Infrastruktur beim AN respektive bei dessen Subunternehmer ist nicht gestattet. Die Sicherungsmaßnahmen gem. § 6 sind zu gewährleisten.

(11) Der AN bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

(12) Der AN verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des AG das Datengeheimnis zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(13) Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigtenverhältnisses in geeigneter Weise zu Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der AN überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften in seinem Betrieb.

(14) Die Liste der Beauftragten für den Datenschutz eines jeden Vertragspartners mit Vorname, Name, Organisation und Telefonnummer ist dem Vertrag zum vHGS nachrichtlich beigefügt.

Ein Wechsel des Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.

§ 6 Mitteilungspflichten des AN bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der AN teilt dem AG unverzüglich Störungen, Verstöße des AN oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des AG nach Art. 33 und Art. 34 DSGVO. Der AN sichert zu, den AG erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den AG darf der AN nur nach vorheriger Weisung gemäß § 4 dieses Vertrages durchführen.

§ 7 Unterauftragsverhältnisse mit Subunternehmern

(1) Der AN ist nach § 3 Abs. 5 vHGS-Vertrag berechtigt zur Erfüllung seiner Leistungen Subunternehmer einzusetzen.

(2) Die Beauftragung von Subunternehmern ist dem AG schriftlich mit Name und Anschrift bekannt zu geben. Der AN versichert, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem AG auf Anfrage zur Verfügung zu stellen.

Der AN hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen AG und AN auch gegenüber Subunternehmern gelten. Insbesondere muss der AG berechtigt sein, im Bedarfsfall angemessene Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der AN hat die Einhaltung der Pflichten aus § 8 dieses Vertrages regelmäßig – mindestens einmal jährlich – zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem AG auf Verlangen zugänglich zu machen.

In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des AN und des Subunternehmers deutlich voneinander

abgegrenzt sind. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach Art. 29 und Art. 32 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der AN haftet gegenüber dem AG dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

Zurzeit sind die in der dem vHGS-Vertrag nachrichtlich beigefügten „Liste mit Subunternehmern der Teilnehmer“ mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der AG einverstanden. Die Liste mit Subunternehmern der Teilnehmer ist immer aktuell zu halten und dem RMV zur Verfügung zu stellen. Mit deren Beauftragung erklärt sich der AG einverstanden.

§ 8 Technische und organisatorische Maßnahmen nach § 9 BDSG

(1) Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzen der AN oder die von ihm beauftragten Dritten das hierfür entwickelte webbasierte mandantenfähige verbundweite Hintergrundsystem (vHGS). Eine Beschreibung der Organisation und Datenverarbeitung sowie des Sicherheitsmanagements im vHGS befindet sich in Anlage 11.

(2) Der AN beachtet die Grundsätze der ordnungsgemäßen Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherungsmaßnahmen.

(3) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen haben die Verantwortlichen und der Auftragsverarbeiter (auch unter Berücksichtigung von UAN) geeignete technische und organisatorische Maßnahmen (TOM) getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen u.a. Folgendes ein:

a) Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Weitere Details dazu wurden in den Datensicherungskonzepten bzw. den TOMs (technische und organisatorische Maßnahmen) der verschiedenen Beteiligten geregelt. Die dort enthaltenen Sicherheitsniveaus sind zwischen dem AN und demjenigen, um dessen Datensicherungskonzept/TOMs es sich handelt, abgestimmt und werden vom AN gewährleistet.

Die nachfolgend aufgeführten Datensicherungskonzepte/TOMs sind verbindlich und werden mit Vertragsabschluss Vertragsbestandteil.

- Anlage 10 (TOMs rms GmbH),
- Anlage 4 (TOMs Technischer Betreiber) und
- Anlage 5 (TOMs Massenpersonalisierer).

AN sowie deren UAN, deren Sicherheitskonzept / TOMs hier nicht ausdrücklich aufgeführt ist, haben mindestens die folgenden Maßnahmen durchzuführen und sicherzustellen:

- Zutrittskontrolle
  Für Verarbeitung der Daten des AG darf das vHGS nur in geschützten Räumen und nur auf Arbeitsplatzrechnern eingesetzt werden, die nach dem Stand der Technik gesichert sind (mindestens vergleichbar zum „Basisschutz für Computer“ des BSI) – d.h. ausreichend gesicherte und mit aktuellen Updates versehene Systemumgebung, Virenschutz, Zugangsschutz durch Benutzerkennung und Passwort sowie sichere Datenablage unter dem Schutz des angemeldeten Benutzerkontos aufweisen. Die Arbeitsumgebung muss gegen missbräuchliche Verwendung und unberechtigte Kenntnisnahme ausreichend geschützt sein.
- Zugangskontrolle
  Der AN stellt sicher, dass Unbefugte über die Arbeitsplatzrechner nicht Einblick oder Zugang zu Daten bekommen – z.B. durch geeignete Aufstellung von Tastatur und Bildschirm. Dies trifft insbesondere auf die Eingabe von Passwörtern zu.
  Der AN stellt sicher, dass jeder Nutzer mit seiner eigenen Benutzer-ID arbeitet und seine Zugangsdaten geheim hält. Nicht mehr benötigte Benutzerkennungen sind unverzüglich zu sperren.
  Bei der Ausgabe von Passwörtern (Initialpasswörter, Ersatzpasswörter nach Rücksetzung) an die Mitarbeiter verhindert der AN wirksam eine unbefugte Kenntnisnahme.
- Zugriffskontrolle
  Die Anzahl der Benutzer ist durch den AN so klein wie möglich zu halten und nicht (mehr) genutzte Benutzer-IDs sind zu löschen. Der AN hat die Rollen restriktiv zu vergeben. Das vHGS setzt ein Benutzer- und Rollenkonzept um: Nur nach Anmeldung mit Benutzername und Passwort kann ein Zugriff auf Daten erfolgen. Aktionen sind nur gemäß der aktuellen Berechtigung des Benutzers möglich. Die Zuordnung von Rollen zu Benutzern wird vom AN so dokumentiert, dass immer der aktuelle Stand ersichtlich ist und vom AG kontrolliert werden kann. Die Vergabe und der Entzug der Berechtigungen (zum Beispiel bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses) werden vom AN regelmäßig kontrolliert und hierfür geeignete Kontrollmechanismen und Verantwortlichkeiten definiert.
- Weitergabekontrolle
  Lokale Kopien von Daten des AG aus dem vHGS sind nicht erlaubt, soweit sie nicht ausdrücklich vom Regelwerk vorgesehen und beschrieben sind. Insbesondere ist nicht erlaubt, gleichzeitig mit dem vHGS andere Software bzw. die Betriebsumgebung des vHGS in einer Konfiguration zu betreiben, die geeignet ist, einen Datenzugriff außerhalb der Sicherheitsmechanismen des vHGS zu ermöglichen.
  Eine Übertragung von Daten an den AG außerhalb des vHGS im Zusammenhang mit der Auftragserfüllung hat ausschließlich über angemessen geschützte und authentifizierte Kanäle zu erfolgen.
  Soweit an den AG übertragene Daten und Unterlagen für Zwecke der Prozesskontrolle vorzuhalten sind, sind diese geschützt und gesperrt aufzubewahren sowie nach vereinbarten Fristen bzw. nach Aufforderung zu vernichten.

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen sind schriftlich zwischen AG und AN zu vereinbaren.

(5) Soweit die beim AN getroffenen Sicherheitsmaßnahmen den Anforderungen des AG nicht genügen, benachrichtigt er den AG unverzüglich.

§ 9 Unterauftragsverhältnisse mit Subunternehmern

Nach Abschluss der vertraglichen Arbeiten hat der AN sämtliche in seinem Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen und/oder datenschutzgerecht zu löschen bzw. zu vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem AG mit Datumsangabe schriftlich zu bestätigen.

§ 10 Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der AG gegenüber dem Betroffenen verantwortlich. Soweit der AG zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim AN vorbehalten, wenn dieser den Schaden vorsätzlich oder fahrlässig verursacht hat. Es gelten die Regelungen des §12 vHGS-Vertrag.

§ 11 Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmern) sind von beiden Vertragsparteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

RHEIN-MAIN-VERKEHRSVERBUND

Technische und organisatorische Maßnahmen Technischer Betreiber

Anlage 4 zum vHGS-Vertrag

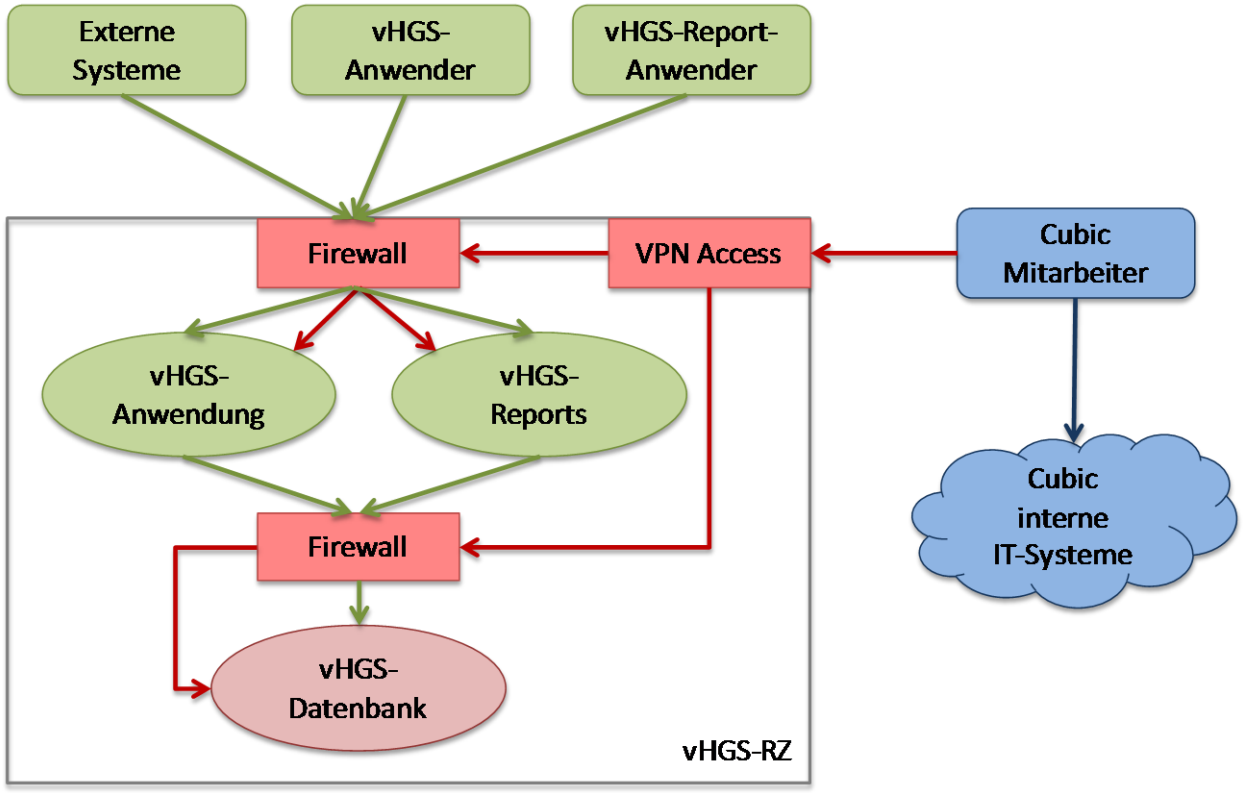
Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	Cubic	08.12.2011	Version als Anlage zum vHGS-Vertrag V1.0
2.2	Cubic	20.09.2012	Version als Anlage zum vHGS-Vertrag V1.0
2.3	Cubic	24.05.2017	Version als Anlage zum vHGS-Vertrag V1.0
2.4	Cubic	14.06.2018	Version als Anlage zum vHGS-Vertrag V1.1

Technische und Organisatorische Maßnahmen

I. Technischer Aufbau des vHGS

Die nachfolgende Abbildung zeigt eine Übersicht über die Struktur des vHGS in Bezug auf den Zugang zum System:



Das vHGS wird in einem Rechenzentrum (vHGS-RZ) betrieben.

Die Mitarbeiter der Mandanten (Verkehrsunternehmen, RMV, rms) greifen als vHGS-Anwender bzw. vHGS-Report-Anwender über Webanwendungen auf Funktionen des vHGS zu. Die vHGS-Datenbank kann auf diesem Weg nie direkt angesprochen werden.

Externe Systeme verwenden Webservice-Schnittstellen, die von der vHGS-Anwendung bereitgestellt werden.

Die Cubic-Mitarbeiter können zum einen als vHGS-Anwender spezielle Funktionen des vHGS nutzen und zum anderen über einen VPN-Zugang direkt auf die Systemkomponenten einschließlich der vHGS-Datenbank zugreifen.

II. Allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen

1. Allgemeine Informationssicherheit und Datenschutzstrategien

Cubic Transportation Systems (Deutschland) GmbH hat allgemeine Informationssicherheits- und Datenschutzstrategien implementiert. Diese werden erreicht durch:

a) Implementierung von Best-Practice-Standards für Informationssicherheit und Datenschutz basierend auf ISO 27002, SOC 2 usw. und / oder Nachweis der Akkreditierung mit einer anerkannten Informationssicherheitszertifizierung (falls zutreffend);

b) Bereitstellung von Informationssicherheits- und Datenschutzschulungen im Rahmen ihrer Informationssicherheits- und Datenschutzprogramms für ihre Mitarbeiter;

c) einen formalen Prozess der Dokumentation, Spezifikation, Prüfung, Qualitätskontrolle und verwalteten Implementierung, wenn neue Systeme implementiert werden oder bestehende Systeme geändert werden (ein Verifizierungstest wird durchgeführt, wenn größere Änderungen an den Systemen stattfinden und solche Verifizierungstests beinhalten auch Sicherheitstests der Änderungen am System).

2. Organisation der Informationssicherheit

Cubic Transportation Systems (Deutschland) GmbH hat eine Managementstruktur und einen Mechanismus zur Koordinierung von Informationssicherheit und Datenschutzaktivitäten implementiert. Diese werden erreicht durch:

a) klar definierte Informationssicherheits- und Datenschutzverantwortlichkeiten innerhalb von Cubic Transportation Systems (Deutschland) GmbH aufgrund von Richtlinien (insbesondere sogenannte Data Protection Governance Policy („Allgemeine Datenschutzrichtlinie“));

b) die erforderliche Informationssicherheit und die Datenschutzkompetenz, die Cubic Transportation Systems (Deutschland) GmbH zur Verfügung stehen, um die hier dargelegten Maßnahmen umzusetzen;

c) die regelmäßige Überprüfung, dass die Verpflichtungen zur Vertraulichkeit oder Geheimhaltung eingehalten.

3. Zugriffskontrolle von Bearbeitungsbereichen

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen ergriffen, um zu verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsgeräten (d.h. Datenbank- und Anwendungsservern und zugehöriger Hardware) erhalten, auf denen personenbezogene Daten verarbeitet werden. Dies wird erreicht durch:

a) Sicherstellung, dass Regeln für die akzeptable Nutzung von Daten im Zusammenhang mit den Informationsverarbeitungseinrichtungen identifiziert, dokumentiert und kommuniziert werden;

b) Einrichtung von Sicherheitsbereichen;

c) Schutz und Einschränkung von Zugriffspfaden;

d) Festlegung von Zugangsberechtigungen für Mitarbeiter und Dritte einschließlich der jeweiligen Dokumentation;

e) Implementierte Vorschriften und Beschränkungen für Zugangsschlüsselkarten und klare Anweisungen im Falle des Verlusts von Zugangsschlüsselkarten;

f) Protokollierung des Zugriffs auf die Rechenzentren, in denen personenbezogene Daten gehostet werden, um eine Überwachung zu ermöglichen;

g) Gesicherte Zugangskontrollen zu den Rechenzentren, in denen personenbezogene Daten gespeichert sind, Sicherheitsalarmsysteme und andere geeignete Sicherheitsmaßnahmen, die Best Practice-Standards entsprechen, um sicherzustellen, dass nur autorisiertes Personal Zugang zu Rechenzentren erhält;

h) 24/7-Wachdienst (24 Stunden, 7 Tage die Woche) in den Rechenzentren, in denen personenbezogene Daten gespeichert sind;

i) Sicherstellung, dass sich externe Besucher an der Rezeption der Rechenzentren registrieren müssen und begleitet werden.

j) Die vertragliche Verpflichtung des Rechenzentrumsdienstleiters PlusServer GmbH, insbesondere durch deren getroffene technischen und organisatorischen Sicherheitsmaßnahmen.

4. Zugriffskontrolle auf Datenverarbeitungssysteme

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen ergriffen, um zu verhindern, dass ihre Datenverarbeitungssysteme von Unbefugten benutzt werden. Dies wird erreicht durch:

a) Identifizierung des Benutzers an dem jeweiligen System;

b) Herausgabe und Sicherung von Zugangsdaten für Benutzer (Passwörter);

c) Verwendung von starken Passwörtern für alle IT-Systeme (d.h. Richtlinien für minimale Zeichen, Komplexitätsregeln und Passwortänderung);

d) Automatisches Ausloggen bei Zeitüberschreitung des Benutzerendgeräts, wenn es im Leerlauf bleibt, wobei die Benutzeridentifikation und das Kennwort zum erneuten Öffnen erforderlich sind;

e) Automatische Sperrung der Benutzeridentifikation, wenn mehrere fehlerhafte Passwörter eingegeben werden, zusammen mit einer Protokolldatei von Ereignissen (Überwachung von Einbruchsversuchen);

f) Deaktivierung der Anmeldeinformationen des Benutzers, die für einen längeren Zeitraum nicht verwendet wurden;

g) Sicherstellung, dass alle Zugangsrechte im Zusammenhang mit personenbezogenen Daten mindestens alle sechs Monate überprüft werden;

h) Sicherstellung, dass alle Benutzeranmeldeinformationen personalisiert sind und nur von der bestimmten Person verwendet werden;

i) Umsetzung eines Verfahrens, dass sicherstellt, dass die Zugriffsrechte der Administratoren kontrolliert werden;

5. Zugangskontrolle zur Nutzung bestimmter Bereiche von Datenverarbeitungssystemen

Cubic Transportation Systems (Deutschland) GmbH hat sich verpflichtet, dass die zur Nutzung seines Datenverarbeitungssystems berechtigten Personen nur im Umfang und in dem Umfang, der durch ihre jeweilige Zugriffsberechtigung (Autorisierung) abgedeckt ist, auf die Daten zugreifen können und dass personenbezogene Daten nicht ohne Genehmigung gelesen, kopiert, verändert oder entfernt werden können. Dies soll erreicht werden durch:

a) Mitarbeiterrichtlinien, klare Anweisungen und Schulungen in Bezug auf die Zugriffsrechte jedes Mitarbeiters in Bezug auf personenbezogene Daten und auf den Umfang der Verarbeitung der personenbezogenen Daten;

b) Sicherstellung, dass sich die Mitarbeiter über die Vertraulichkeitspflichten in Bezug auf personen-

bezogene Daten im Klaren sind;

c) Sicherzustellen, dass es jederzeit möglich ist, die Namen und Kontaktinformationen (wie z.B. Telefonnummer und E-Mail-Adresse) aller Mitarbeiter und anderer Personen, die Zugang zu bestimmten personenbezogenen Daten haben, festzustellen;

d) Wirksame und angemessene Disziplinarmaßnahmen gegen eigene Mitarbeiter, die unbefugt auf personenbezogene Daten zugreifen;

e) Einführung einer Autorisierungsrichtlinie für den Zugang und die Eingabe von personenbezogenen Daten in Systeme und Anwendungen sowie für das Lesen, Ändern und Löschen gespeicherter personenbezogener Daten;

f) Gewährleistung, dass der Zugang zu personenbezogenen Daten nur autorisierten Personen auf der Grundlage der Notwendigkeit ("need-to-know") zur Verfügung gestellt wird;

g) dass keine personenbezogenen Daten in Dateien, auf Papierkopien oder anderen verkörperlichten Medien dauerhaft vorhanden sind und dadurch das Kopieren, Reproduzieren oder Löschen für unbefugte Personen dieser Daten verhindert wird;

h) Benutzerrechtemanagement innerhalb der Anwendung (vHGS), das sicherstellt, dass Anwender 1) nur die für Ihre Organisation freigegebenen Daten anzeigen/bearbeiten können und 2) nur die für Ihre Tätigkeit benötigten Daten anzeigen/bearbeiten können.

6. Steuerung der Übermittlung

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen getroffen, um zu verhindern, dass personenbezogene Daten von Unbefugten während deren Übermittlung oder beim Transport der Datenträger gelesen, kopiert, verändert oder gelöscht werden. Dies wird erreicht durch:

a) Einsatz von Firewalls- und Verschlüsselungstechnologien zum Schutz der Gateways und Pipelines, durch die sich die Daten bewegen;

b) Kein Erfordernis der Speicherung personenbezogener Daten auf mobilen Speichermedien zu Transportzwecken;

7. Steuerung der Eingabe/Erfassung

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen ergriffen, um sicherzustellen, dass geprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben oder gelöscht wurden. Dies wird erreicht durch:

a) Umsetzung einer Autorisierungsrichtlinie zum Lesen, Ändern und Löschen gespeicherter Daten;

b) Authentifizierung von autorisiertem Personal;

c) Protokollierung von Datenänderungen innerhalb der Anwendung;

8. Jobkontrolle

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen ergriffen, um sicherzustellen, dass im Falle einer Auftragsverarbeitung (gemäß Artikel 28 DS-GVO) personenbezogener Daten, die personenbezogenen Daten gemäß den Anweisungen von Cubic Transportation Systems (Deutschland) GmbH verarbeitet werden. Dies wird erreicht durch:

a) Sorgfältig ausgewählte Bearbeiter (Diensteanbieter, die personenbezogene Daten im Auftrag von Cubic Transportation Systems (Deutschland) GmbH verarbeiten);

b) Sicherstellung klarer Anweisungen bezüglich des Umfangs der Verarbeitung personenbezogener Daten im Auftrag;

c) Effektive Prüfungsrechte, die mit den Verarbeitern vereinbart wurden;

d) Vereinbarungen zur Auftragsverarbeitung mit weiteren Verarbeitern (Subunternehmern).

9. Trennung der Verarbeitung für verschiedene Zwecke

Cubic Transportation Systems (Deutschland) GmbH hat geeignete Maßnahmen implementiert, um sicherzustellen, dass Daten, die für verschiedene Zwecke gesammelt werden, getrennt verarbeitet werden können. Dies wird erreicht durch:

a) Der getrennte Zugriff auf Daten erfolgt durch Anwendungssicherheit für die entsprechenden Benutzer;

b) Module sind innerhalb der Datenbanken nach Zweck getrennt (d.h. nach Funktionalität und Funktion), wenn personenbezogene Daten verarbeitet werden;

c) Speicherung von personenbezogenen Daten auf der Datenbankebene in verschiedenen normalisierten Tabellen;

d) Schnittstellen, Batch-Prozesse und Berichte sind nur für bestimmte Zwecke und Funktionen ausgelegt, so dass für bestimmte Zwecke erhobene Daten getrennt verarbeitet werden.

10. Pseudonymisierung

Cubic Transportation Systems (Deutschland) GmbH hält folgende Sicherheitsmaßnahmen ein, um die Pseudonymisierung der personenbezogenen Daten gewährleisten zu können:

a) Die Verarbeitung personenbezogener Daten erfolgt nach Möglichkeit so, dass die Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können.

b) Verwendung von Best-Practice-Pseudonymisierungstechnologien..

11. Verschlüsselung

Cubic Transportation Systems (Deutschland) GmbH hält die folgenden Sicherheitsmaßnahmen ein, um die Verschlüsselung der personenbezogenen Daten gewährleisten zu können:

Verschlüsselung der personenbezogenen Daten während der Übertragung nach dem aktuellen Stand der Technik.

12. Vertraulichkeit der Verarbeitungssysteme und der Dienstleistungen

Cubic Transportation Systems (Deutschland) GmbH hält die folgenden Sicherheitsmaßnahmen ein, um die Vertraulichkeit der Verarbeitungssysteme und der Dienste gewährleisten zu können:

Siehe Abschnitte zur Zugriffskontrolle Nr. 3., 4., 5. und Abschnitt über die Verschlüsselung Nr. 11. oben.

13. Integrität der Verarbeitungssysteme und der Dienste

Cubic Transportation Systems (Deutschland) GmbH hält die folgenden Sicherheitsmaßnahmen ein, um die Integrität der Verarbeitungssysteme und der Dienste zu gewährleisten:

a) Sicherstellung, dass die Verarbeitungssysteme (wie etwa Software, Hardware, einschließlich Netzwerkinfrastruktur) durch geeignete Mittel (z.B. Antivirensoftware, Softwareaktualisierungen, Firewalls) vor Manipulation oder Zerstörung geschützt sind;

b) Installation von Diensten oder Software zu verbieten, die schädlich für die Verarbeitungssysteme, die Dienste oder den Umgang mit personenbezogenen Daten sind;

c) siehe auch Abschnitte zu Zugangskontrollen Nr. 3., 4., 5. und Abschnitt über die Verschlüsselung Nr. 11. oben.

14. Verfügbarkeit der Verarbeitungssysteme und der Dienste sowie Fähigkeit zur zeitnahen Wiederherstellung der Verfügbarkeit und des Zugangs zu den personenbezogenen Daten im Falle eines physischen oder technischen Ereignisses

Cubic Transportation Systems (Deutschland) GmbH hält die folgenden Sicherheitsmaßnahmen ein, um die Verfügbarkeit der Verarbeitungssysteme sicherzustellen und die Verfügbarkeit und den Zugriff auf die persönlichen Daten bei einem physischen oder technischen Ereignis (einschließlich der Sicherstellung der Sicherheit) rechtzeitig wiederherstellen zu können, so dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

a) Richtlinien zur Kontrolle der Aufbewahrung von Sicherungskopien und der Wiederherstellung verlorener oder gelöschter Daten;

b) Infrastrukturredundanz (einschließlich unterbrechungsfreier Stromversorgung) und periodische Funktionstests;

c) Physischer Schutz von IT-Ressourcen;

d) Umfassendes Monitoring mit automatischer Alarmierung (24/7 Rufbereitschaft) bei Nichtverfügbarkeit der Anwendung oder unerwartetem Systemverhalten;

e) Redundante Speicherung der Datenbankinhalte (Live-Datenbank und Standby-Datenbank) in einem in sich redundanten Storage (RAID) sowie Erzeugung von Sicherungskopien auf einem unabhängigen Datenträger im gleichen Rechenzentrum;

f) Handhabung von Sicherungskopien mit der gleichen Vertraulichkeit wie die ursprünglichen persönlichen Daten;

g) Sicherungskopien (Backups der Datenbank) werden für mindestens 3 Wochen, maximal 12 Wochen aufbewahrt;

h) Geschäftskontinuitätspläne.

15. Belastbarkeit der Verarbeitungssysteme und der Dienstleistungen

Cubic Transportation Systems (Deutschland) GmbH hält die folgenden Sicherheitsmaßnahmen ein, um die Ausfallsicherheit der Verarbeitungssysteme und der Dienste zu gewährleisten:

a) Systeme und Netzwerke werden auf konsistente und genaue Weise mit genehmigten Sicherheitseinstellungen konfiguriert, um sicherzustellen, dass Systeme und Netzwerke wie gewünscht funktionieren, bei Bedarf verfügbar sind und keine unnötigen technischen Details offenlegen;

b) Netzwerkredundanz (sowohl RZ-intern als auch externe Anbindung des RZ);

c) Verwendung in sich redundant aufgebauter Hardware (Storage, Server).

16. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbei-

tung

Cubic Transportation Systems (Deutschland) GmbH behält den folgenden Prozess bei, um die Wirksamkeit der technischen und organisatorischen Maßnahmen von Cubic Transportation Systems (Deutschland) GmbH zur Gewährleistung der Sicherheit der Datenverarbeitung regelmäßig zu testen, zu bewerten und zu beurteilen:

a) Das Informationssicherheits-Team von Cubic in Großbritannien führt wöchentlich Scans mit Nessus Vulnerablity Checker durch;

b) Tägliche / wöchentliche / monatliche Auswertung zur erreichten Systemverfügbarkeit;

c) Monatliche Besprechung über Status und Auffälligkeiten des RZ-Betriebs mit dem Betreiber der RZ-Infrastruktur;

d) Anlassbezogene Erstellung von Störungsberichten (Hergang, Sofortmaßnahmen, Verbesserungsmaßnahmen).

III. Datenkategorien und Löschfristen

Grundsätzlich gilt für alle gespeicherten Daten das Prinzip der Datensparsamkeit. Das bedeutet zum einen, dass nur die Daten erhoben werden dürfen, die unbedingt für die Ausführung des Dienstes notwendig sind. Zum anderen heißt das aber auch, dass die Daten nur so lange wie nötig im System vorgehalten werden dürfen.

Alle vom vHGS gespeicherten Daten werden einer Kategorie zugeordnet. Die folgende Tabelle führt die Kategorien auf, erläutert, warum sie erhoben werden, und spezifiziert, wie und wann sie wieder entfernt werden.

Kategorie	Datenart	Datenelemente	Grund der Datenhaltung	Behandlung/ Verfahren	Frist
LOGGING	Teils Dateien in Textform (Logfiles), teils Datenbankeinträge (Access Log)	Detaillierte Beschreibungen der Verarbeitungsschritte und evtl. auftretender Fehlersituationen.	Technische Problemlösung Sicherheitsanaly-sen	Löschung nach definierter Frist.	3 Monate
VERKAUF	Datenbank-einträge	Detaildatensätze der Verkaufstransaktionen	Nachweise entsprechend AGB/ABB, Grundlage der Rechnungsstellung	Löschung nach definierter Frist	Fallabschluss + 6 Monate
KUNDE	Datenbank-einträge	Detaildaten (Name, Adresse, …) zur Person des Kunden	Nachweise entsprechend AGB/ABB, Grundlage der Rechnungsstellung	Löschung nach definierter Frist	Fallabschluss + 6 Monate
FINANZ	Datenbankeinträge	Verträge (Abo, …)	Grundlage der Rechnungsstellung, Ausweis gegenüber Steuerbehörde	Löschung nach definierter Frist, nach Archivierung aufbewahrungspflichtiger Daten	Fallabschluss + 6 Monate Archiv Vertragsdaten: 10 Jahre
	Datenbank-einträge	Rechnungen und Bezahltransaktionen	Ausweis gegenüber Steuerbehörde	Löschung nach definierter Frist, nach Archivierung aufbewahrungspflichtiger Daten	Fallabschluss + 6 Monate Archiv Rechnungsdaten: 10 Jahre
	Datenbank-einträge	Sortennachweise (enthalten keine Kundendaten)	Ausweis gegenüber Wirtschaftsprüfer Statistik	Löschung nach definierter Frist	10 Jahre

Kategorie	Datenart	Datenelemente	Grund der Datenhaltung	Behandlung/ Verfahren	Frist
SPERR-LISTEN	Datenbank-einträge	Kartennummern, Fahrkarten, die auf-grund einer Regel-verletzung ausge-schlossen wurden	Schutz der Unter-nehmen vor Ein-nahmeausfällen.	Löschung nach definierter Frist	Fallabschluss + 3 Monate
KONTROLLE	Datenbank-einträge	Daten von Kontroll- und Sperrnachwei-sen	Sperrmanagement Auswertungen für Betrugsverdachts-analyse	Analyse der Daten und an-schließend Löschung	min. 3 Tage, max. 14 Tage

Hinweis zu Daten aus der Kontrolle von eTickets

In den bei der Kontrolle von eTickets entstehenden KA-Transaktionsnachweisen vom Typ TXEBER (059) werden bei Eingang im vHGS folgende Felder des Datenbereichs „AllgemeineFahrttransaktionsdaten“ mit „0“ (oder anderslautenden nichtinformationstragenden Werten) überschrieben:

- fahrtNummer
- berLogLinieVarianteID.linieID
- berLogLinieVarianteID.varianteNummer

RHEIN-MAIN-VERKEHRSVERBUND

Technische und organisatorische Maßnahmen
Massenpersonalisierer

Anlage 5 zum vHGS-Vertrag

RHEIN-MAIN-VERKEHRSVERBUND

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	ComCard	27.08.2009	Version als Anlage zum vHGS-Vertrag V1.0
1.1	SPS	01.03.2016	Version als Anlage zum vHGS-Vertrag V1.0
2.1	TCS	19.07.2017	Version als Anlage zum vHGS-Vertrag V1.0
4	TCS	19.06.2018	Version als Anlage zum vHGS-Vertrag V1.1

GNC&TCS

Übersicht der technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO

1. Pseudonymisierung und Verschlüsselung (Art.32 Abs.1a; Art.25 Abs. 1 DSGVO)

Zu gewährleisten, dass die Daten, ohne Hinzuziehung zusätzlicher Informationen, nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Es werden kryptographische Verfahren, wie AES und RSA Verschlüsselungsalgorithmen eingesetzt.

2. Sicherstellung der Verarbeitung

2.1. Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

2.1.1. Zutrittskontrolle

Unbefugten den Zutritt zu solchen Datenverarbeitungsanlagen *zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen.*

- Ausschließlich zutrittsberechtigte Personen gelangen auf das Firmengelände oder in das Firmengebäude.
- Alle Personalzugangstüren und Vereinzelungsanlagen sind mit Zutrittskontrolllesern und Überwachungskameras gesichert.
- Regelungen für Besucher, Lieferanten und Wartungspersonal sind vorhanden. Die Registrierung aller externen Personen erfolgt auf Besucherscheinen und Kfz-Einfahrtslisten durch Mitarbeiter der Sicherheitszentrale. Eine Identitätsfeststellung ist jederzeit anhand von Besucher- und Handwerkerausweisen möglich.
- Vergabe von Zutrittsberechtigungen ausschließlich nach dem Need-To-Know-Prinzip.
- Fremdkräfte (z.B. Wartungspersonal) sind nur mit Genehmigung, Protokollierung und Aushändigung besonderer Ausweise in Sicherheitsbereiche mit Datenverarbeitung zugangsberechtigt. Sie sind grundsätzlich in Begleitung.
- Zutrittsberechtigte Personen sind eindeutig bekannt und die Personalbewegungen werden protokolliert.
- Die unterschiedlichen Sicherheitsbereiche sind nur mit Key-Card begehbar. Sensible Bereiche nur im 4 Augenprinzip, Key-Card und Ziffern-Code.
- Zutrittsberechtigungen werden nach einer von der Geschäftsleitung vorgegebenen Rollenmatrix vergeben.
- Alle Hochsicherheitsbereiche sind automatisch gesicherte Scharfschaltebereiche.
- Außerhalb der Produktions- und Bürozeiten werden die Produktionsräume bzw. das Gebäude alarmgesichert.
- Schlüssel/Schlüsselvergaben werden vom Sicherheitsmanagement verwaltet und überwacht.

2.1.2. Zugangskontrolle

Zu verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Kritikalitätsabhängige Netzwerksegmentierung mit mehrstufigen Firewall-Systemen.
- Produktionsbereiche ohne Internetzugang
- Vergabe von Zugangsberechtigungen ausschließlich nach dem Need-To-Know-Prinzip.
- Zugangsberechtigungen werden nach einer von der Geschäftsleitung vorgegebenen Zutritts-/Rollenmatrix vergeben.
- Die Zugangsberechtigungen sind zentral innerhalb Active Directory verwaltet.

Erstellt: Günter Wolf	Geprüft: CISO/DSBm	Freigabe: GF	Revisionsstand: 4
am: 16.11.2009m	am: 27.11..2017m	am: 27.11.2017m	Internal use onlym
Revision: Michael Priester	Geprüft CISO/DSB		
am 19.06.2018	19.06.2018		

- Die Vergabe von Berechtigungen erfolgt mittels schriftlicher Anweisung und Freigabe durch den jeweiligen Vorgesetzten.
- Ein geregeltes Kennwortverfahren existiert. Minimale Kennwortlänge 8 Zeichen. Das Kennwort muss den Komplexitätsanforderungen von Microsoft entsprechen (mindestens 3 von 4 Kennwortkategorien, wie z. B. Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen). Kritikalitätsabhängiges maximales Kennwortalter 30 – 90 Tage.
- Sperrung des Kontos nach 3, bzw. kritikalitätsabhängig bis maximal 5, Fehlversuchen.
- Aktivierung Bildschirmschoner mit Kennwortschutz bei Passivität kritikalitätsabhängig nach 5 bis maximal 15 Minuten.
- Richtlinie Datenklassifizierung regelt u.a. die Verschlüsselung von Datenträgern.

2.1.3. Zugriffskontrolle

Zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegende Daten zugreifen können.

- Zugriffsberechtigungen werden nach einer von der Geschäftsleitung vorgegebenen Rollenmatrix vergeben.
- Vergabe von Zugriffsberechtigungen ausschließlich nach dem Need-To-Know-Prinzip.
- Es existieren definierte Verfahren für die Vergabe, Änderung und Löschung von Zugriffsberechtigungen
- Es existiert ein definierter Change-Management-Prozess.
- Es existieren definierte, regelmäßige Auswertungen und Überprüfungen der existierenden Zugriffsberechtigungen.
- Es existieren definierte, regelmäßige Auswertungen und Überprüfungen von Logfiles.

2.1.4. Trennungskontrolle

Zu gewährleisten, dass zu unterschiedlichen Zwecken Daten getrennt verarbeitet werden können.

- Es existiert eine logisch getrennte Datenverwaltung (Mandant; Auftragsnummer) um zu gewährleisten, dass Daten weisungsgemäß verarbeitet werden
- Es existiert eine logisch und physikalisch getrennte Test- und Produktivumgebung.

2.2. Integrität (Art. 32 Abs. 1b DSGVO)

2.2.1. Weitergabekontrolle

Zu gewährleisten, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Richtlinie Datenklassifizierung und die Verfahrensanweisung Vertraulichkeit der Information regeln die Maßnahmen zum Schutz der Daten bei Übertragung, Transport, Speicherung und Übermittlung.
- Richtlinie Kryptographie regelt die zum Einsatz geeigneten Verschlüsselungsalgorithmen und Verfahren. Die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) finden Anwendung.
- Eine Datenverschlüsselung während der Übertragung ist obligatorisch.
- Datenträger werden nur an autorisierte Personen mit Begleitpapieren ausgegeben. Die Lagerung erfolgt im Tresorraum oder im Tresor der IT-Abteilung.
- Alle Datenübertragungen werden protokolliert. Bei Dateneingang werden diese auf Vollständigkeit und Richtigkeit überprüft.

Erstellt: Günter Wolf	Geprüft: CISO/DSBm	Freigabe: GF	Revisionsstand: 4
am: 16.11.2009m	am: 27.11..2017m	am: 27.11.2017m	Internal use onlym
Revision: Michael Priester	Geprüft CISO/DSB		
am 19.06.2018	19.06.2018		

GNC&TCS

2.2.2. Eingabekontrolle

Zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Durch Protokollierung kann nachvollzogen werden, welche Eingaben zuletzt gemacht wurden.
- Einsatz von Log-Server im Produktionsbereich.
- Definierte Maßnahmen zum Schutz von Protokollinformationen sind umgesetzt.
- Es existieren definierte, regelmäßige Auswertungen und Überprüfungen von Logfiles.

2.2.3. Löschgebot

Zu gewährleisten, dass die Daten datenschutzgerecht und nicht wieder herstellbar gelöscht werden. Daten in Datenbanksystemen sind so aus der logischen Struktur zu löschen, dass die Löschung nicht rückgängig gemacht werden kann.

- Die Datenlöschung erfolgt automatisiert. Daten, die im Hochsicherheits-Netzwerk verarbeitet/gespeichert sind, werden nach 30 Tagen gelöscht. Alle anderen Daten nach 90 Tagen. Ausnahmen können aus Kundenauflagen resultieren (Datenlöschung mittels Software).
- Die Datenträgervernichtung erfolgt kontrolliert nach den Richtlinien der Materialklassifizierung.
  - Physikalische Zerstörung der Datenträger
  - Shreddern von Karten gem. PCI CP Standard
  - Shreddern von papierhaften Unterlagen (z.B. Vernichtung nach DIN 66399 (mindestens Sicherheitsstufe P4)
- Obligatorisch ist die Dokumentation der Vernichtung von Datenträger.
  - u.a. Datum der Löschung/Zerstörung/Vernichtung
  - Mitarbeiter der die Löschung/Zerstörung/Vernichtung durchgeführt hat
  - Art des Datenträgers/Speichermediums

2.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1b DSVGO)

2.3.1. Verfügbarkeitskontrolle

Zu gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Kritische Prozesse sind auf Basis Business Impact Analyse und Risikomanagement identifiziert.
- Kritikalitätsabhängig kommen Schutzmechanismen wie „Redundant Array of Independent Disks“ (RAID-Systeme) oder redundante IT-Systeme in gesicherter Umgebung zum Einsatz.
- Backup-Verfahren (D2D2T und D2T) im Einsatz, welche sich je nach Schutzbedarf in der zeitlichen Wiederholung von mehrmals am Tag über täglich bis wöchentlich bewegen.
- Aufbewahrung von Archivierungsbändern in speziellem Tresor bzw. Tresorschrank in einem separaten Brandabschnitt.
- Zentral gemanagter und überwachter Virenschutz
- Business Impact relevante IT-Systeme sind an eine zentrale USV angeschlossen.
- Zusätzliche Notstromversorgung durch zentralen Dieselgenerator.
- Die Serverräume sind mit Inergen-Löschanlagen gesichert.
- Das gesamte Gebäude ist mit einer Brandmeldeanlage mit Brandfrüherkennung ausgerüstet, die parallel auf die ständig besetzte Wache der Feuerwehr Bamberg und auf die Notrufzentrale eines externen Wachunternehmens geschaltet ist.
- Die Serverschränke in den Serverräumen haben Sensoreinheiten zur Überwachung von Rauch, Luftfeuchtigkeit, Luftstrom und Temperatur. Bei Störung erfolgt eine Benachrichtigung via SMS Meldung.
- Es existiert ein dokumentiertes Notfallkonzept.

Erstellt: Günter Wolf	Geprüft: CISO/DSBm	Freigabe: GF	Revisionsstand: 4
am: 16.11.2009m	am: 27.11..2017m	am: 27.11.2017m	Internal use onlym
Revision: Michael Priester	Geprüft CISO/DSB		
am 19.06.2018	19.06.2018		

3. Rasche Wiederherstellung der Verfügbarkeit und Zugang bei einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1c DSVGO)

- Desaster Recovery Plan
- Wieder-Anlauftests
- Backups-Restore-Tests
- Backup-Management

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art.32 Abs. 1d; Art 25 Abs. 1 DSGVO)

Allgemein:

- Zertifizierung nach DIN EN ISO 9001
- Zertifizierung nach DIN EN ISO 27001
- Zertifizierung PCI CP durch Master Card und Visa

4.1. Auftragskontrolle

Zu gewährleisten, dass Daten, die im Auftrag verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet oder genutzt werden können.

- Verträge und Auftragsbestätigungen liegen schriftlich vor und beinhalten alle Aufgaben und Pflichten von Auftraggeber und Auftragnehmer.
- Aus den Angebots-/Vertragsunterlagen wird über die Bestellung des Kunden durch die Mitarbeiter der Arbeitsvorbereitung der Auftrag angelegt. Darin enthalten sind alle am Prozess beteiligten, auftragsbezogenen Materialien und Arbeitsschritte.
- Das Auftragsmanagement überprüft die Angaben aus dem Auftrag mit der Bestellung bzw. dem Vertrag des Kunden und legt einen internen Betriebsauftrag an.
- Für die einbezogenen Abteilungen gibt es detaillierte Auftragsunterlagen, nach denen sich die Produktion richten muss, z. B. Betriebsauftrag, Musterstandvorgaben, Layouts etc.
- Spezielle Anforderungen des Kunden werden mit den am Produktionsprozess beteiligten Abteilungen besprochen.
- Besteht die Notwendigkeit, so werden spezielle Arbeits-, Verfahrens-, Prüf-, und Sicherheitsanweisungen erstellt.
- Im Rahmen des QM-Systems werden die Arbeitsergebnisse regelmäßig durch Qualitätsaufzeichnungen der Produktion, Stichproben des QM-Teams, sowie interne und externe Audits überprüft.
- Weiterhin werden die Sicherheitsanforderungen der Kunden durch ein eigenes implementiertes Sicherheitsmanagementsystem überwacht. Externe sowie interne Audits gewährleisten das hohe Sicherheitsniveau der TCS Cards & Services GmbH, welches ständig modifiziert wird.
- Es existiert eine logisch getrennte Datenverwaltung (Mandant; Auftragsnummer) um zu gewährleisten, dass Daten weisungsgemäß verarbeitet werden.
- Es gibt nur Weiterverarbeitungsprogramme für Auftraggeber, mit denen eine vertragliche Regelung über die Verarbeitung existiert.
- Es existiert ein dokumentiertes Verfahren zur Lieferantenauswahl und Bewertung.

Erstellt: Günter Wolf	Geprüft: CISO/DSBm	Freigabe: GF	Revisionsstand: 4
am: 16.11.2009m	am: 27.11..2017m	am: 27.11.2017m	Internal use onlym
Revision: Michael Priester	Geprüft CISO/DSB		
am 19.06.2018	19.06.2018		

RHEIN-MAIN-VERKEHRSVERBUND

Konzept Externer Mandant

Anlage 6 zum vHGS-Vertrag

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.4	Cubic	08.11.2011	Version als Anlage zum vHGS-Vertrag V1.0

Inhalt

1 Einleitung

Die Verkehrsunternehmen VGF und HEAG verwenden für Vertrieb des eTicket RheinMain nicht das vHGS als KVP- bzw. DL-Referenzsystem (logische Referenzsysteme im Standard der VDV Kernapplikation), sondern eigene eTicket Hintergrundsysteme. Im Konzept „Externer Mandant“ werden die in diesem Zusammenhang getroffenen Vereinbarungen für die Verknüpfung mit Prozessen des vHGS dokumentiert. Grundsätzlich ist die Lösung nicht auf die genannten Unternehmen beschränkt. Da eine Ausweitung des Konzeptes aber nicht geplant ist, werden die beiden relevanten Unternehmen konkret benannt.

2 Aufgabenstellung

Es ist geplant, dass diese Hintergrundsysteme im Sommer 2012 über eine bidirektionale Schnittstelle mit dem vHGS verbunden werden, so dass die VGF und HEAG als Teilnehmer der RMV KVP-Agentur in das verbundweite Servicekonzept eingebunden sind. Das technische Konzept dieser bidirektionalen Schnittstelle zur Synchronisation der Daten im vHGS mit denen im jeweiligen VU-HGS wurde im März 2011 zwischen den Beteiligten grob skizziert und soll im Januar 2012 wieder aufgenommen werden. Damit hat das vorliegende Dokument für die Zeit vom Systemstart des eTicket RheinMain zum Fahrplanwechsel 2012 bis zur Herstellung der Betriebsbereitschaft der bidirektionalen Schnittstelle einen temporären Charakter.

Für den oben genannten Übergangszeitraum soll ein eingeschränkter Datenaustausch zwischen dem vHGS und den Hintergrundsystemen (VU-HGS) der VGF und der HEAG hergestellt werden. Der Datenaustausch erfolgt mittels KA Transaktionsdatensätzen (KA Version 1.107).

Um die Aufwände für die Implementierung zu begrenzen soll die zum Systemstart verwendete Schnittstelle zwischen vHGS und VU-HGS sich auf die für das Sperrmanagement und das Aktionsmanagement zwingend erforderlichen Daten beschränken.

Daten über ausgegebene Nutzermedien und Berechtigungen werden nicht übermittelt. Erst mit dem Betriebsstart der bidirektionalen Schnittstelle werden die seit dem Systemstart angefallenen Daten von den VU-HGS an das vHGS übermittelt.

Für die von VGF und HEAG ausgegebenen Nutzermedien (KA Nutzermediumapplikation) und eTickets (KA Berechtigung, RMV EFS) wird es bis zur Herstellung der Betriebsbereitschaft der bidirektionalen Schnittstelle keinen unternehmensübergreifenden Service (Service durch Dritte) geben. Umgekehrt werden auch die von den vHGS-Mandanten ausgegebenen Nutzermedien und eTickets bei der VGF und HEAG keinen Service durch Dritte erhalten.

Um nach Herstellung der Betriebsbereitschaft der bidirektionalen Schnittstelle eine schnelle Migration ohne Austausch von Nutzermedien und eTickets zu ermöglichen, sollen VGF und HEAG bereits ab dem Systemstart die KVP-ID der RMV KVP-Agentur verwenden. Sie werden daher in diesem Konzept als Externe Mandanten bezeichnet.

Die Verwendung der KVP-ID der RMV KVP-Agentur (und des damit einhergehenden Schlüsselmaterials) wirkt sich auch günstig auf die Einbindung der VGF und der HEAG in das Aktionsmanagement des eTicket RheinMain aus (In einer Lösung mit jeweils eigenen KVP-ID für VGF und HEAG wäre es notwendig, dass die Terminals das Nachladen von Schlüsseln und die Verwendung von „Fremd“-Schlüsseln als ausführender KVP beherrschen – beides wird derzeit von den VU-HGS der VGF und der HEAG nicht unterstützt).

Die Verwendung der KVP-ID der RMV KVP-Agentur durch externe Systeme (ohne Datensynchronisation im Sinne der bidirektionalen Schnittstelle) erfordert Softwareanpassungen im vHGS. Der Grund dafür liegt darin, dass alle bisherigen Konzepte zur Steuerung der Datenverarbeitung im vHGS darauf aufbauten, dass die RMV KVP-Agentur von den Mandanten des vHGS gebildet wird.

3 Lösungskonzept

3.1 Vorbemerkung: Stellvertreter-AHS und KOSES

Bei der Gestaltung der Schnittstelle ist folgender, allgemein für das vHGS geltender Sachverhalt zu berücksichtigen:

Durch die eingetretenen Verzögerungen (gemessen an den Projektplänen im Sommer 2010) bei der abschließenden Detailspezifikation der Schnittstelle („ION-Schnittstelle“) zur zentralen Vermittlungsstelle durch die VDV KA-KG und ATOS, wird das vHGS zum Systemstart die zentrale Vermittlungsstelle nicht nutzen. Auf Seiten des vHGS werden Maßnahmen ergriffen, um dies zu kompensieren. Dies beinhaltet unter anderem:

- Es wird ein „Stellvertreter-AHS“ implementiert, das zum einen vom vHGS die TXAA, TXRA und TXSNAWA erhält und speichert, zum anderen Sperranfragen für SAMs und Organisationen entgegennimmt.
- Es wird ein „Stellvertreter-AH-KOSES“ implementiert, so dass für das eTicket RheinMain ein vollständiges Sperrmanagement für Berechtigungen, Nutzermediumapplikationen, Schlüssel, SAMs und Organisationen vorhanden ist.

- Die in den o.g. „Stellvertreter“-Systemen gespeicherten Daten können im Zuge der späteren Integration mit den zentralen Systemen der VDV-KA KG verwendet werden, um dort als historische Daten eingespielt zu werden.

3.2 Datenflüsse (KA Transaktionsdatensätze)

Die Schnittstelle zwischen vHGS und VU-HGS soll sich auf die für das Sperrmanagement und das Aktionsmanagement zwingend erforderlichen Daten beschränken. D.h.

- Sperrmanagement – Berechtigungen (RMV-EFS)

  Jedoch ohne Sperranfragen und Sperraufhebungsanforderungen. Sofern es einen Bedarf gibt, eine fremde Berechtigung zu sperren, muss die Sperranfrage organisatorisch (Telefon, E-Mail) übermittelt werden.

- Sperrmanagement – NmApplikation (eTicket RheinMain Nutzermedium)

  Jedoch ohne Sperranfragen und Sperraufhebungsanforderungen. Sofern es einen Bedarf gibt, ein fremdes Nutzermedium zu sperren, muss die Sperranfrage organisatorisch (Telefon, E-Mail) übermittelt werden.

- Sperrmanagement – KEY

  Jedoch ohne Sperranfragen und Sperraufhebungsanforderungen. Sofern es einen Bedarf gibt, einen fremden Sicherheitsschlüssel zu sperren, muss die Sperranfrage organisatorisch (Telefon, E-Mail) übermittelt werden.

- Sperrmanagement – SAM, ORG

  Jedoch ohne Sperranfragen und Sperraufhebungsanforderungen.

  Sperranfragen und Sperraufhebungsanforderungen für SAMs und ORGs sind von der VGF bzw. HEAG per E-Mail oder Fax an die übergeordnete fachliche Betriebsführung (üfB) des vHGS (vgl. Anlage 2 „Regelwerk vHGS“, Kap. 2.2 u. 3) zu richten.

  Sperraufträge für SAMs und ORGs werden gemäß KA Spezifikation vom AH erstellt. Für das AH-Stellvertretersystem ist dies so gelöst, dass das AH-Stellvertretersystem auf eine Sperranfrage SAM bzw. ORG immer einen entsprechenden Sperrauftrag erzeugt.

- Aktionsmanagement (RMV-EFS)

Nachfolgend sind die auszutauschenden KA Transaktionsdaten tabellarisch dargestellt. Bzgl. der Kennzeichnung als „synchron“ / „asynchron“ siehe Kap. 3.4.

3.2.1 Sperrmanagement – Berechtigungen (RMV-EFS)

vHGS als KOSE		**VU-HGS als KVP**
	<< TXSAUFB << asynchron	Sperrauftrag für eine vom VU ausgegebene Berechtigung (RMV-EFS)
	<< TXSFREIB << asynchron	Sperrfreigabeauftrag für eine vom VU ausgegebene Berechtigung (RMV-EFS)
vHGS als KOSE		**VU-HGS als KVP oder DL**
TXAS auswerten und TXSLNM zurückliefern	<<TXAS << >> TXSLNM >> synchron	Abruf der Sperrliste NM

	<< TXSNAWB << asynchron	BER-Sperrnachweis aus BER-Sperren einreichen.
vHGS als PV		**VU-HGS als KVP**
BER-Sperrnachweis aus BER-Sperren an den KVP der Berechtigung weitergeben.	>> TXSNAWB >> asynchron	

3.2.2 Sperrmanagement – NmApplikation (eTicket RheinMain Nutzermedium)

vHGS als KOSE		**VU-HGS als KVP**
	<< TXSAUFA << asynchron	Sperrauftrag für eine vom VU ausgegebene NmApplikation (Nutzermedium)
	<< TXSFREIA << asynchron	Sperrfreigabeauftrag für eine vom VU ausgegebene NmApplikation (Nutzermedium)
	<< TXSNAWA << asynchron	APP-Sperrnachweis aus APP-Sperre einreichen.
Nach Anforderung (TXAS) die APP-Sperrnachweise aus APP-Sperren einzeln an den KVP der NmApplikation senden.	<< TXAS << >> TXSNAWA >> … asynchron, siehe Kap. 3.3.5	APP-Sperrnachweise anfordern.
vHGS als KOSE		**VU-HGS als KVP oder DL**
TXAS auswerten und TXSLNM zurückliefern *Redundant zu dem Abruf der TXSLNM in „Sperrmanagement – Berechtigungen“.*	*<<TXAS << >> TXSLNM >> synchron*	*Abruf der Sperrliste NM*
	<< TXSNAWA << asynchron	APP-Sperrnachweis aus APP-Sperre einreichen.

3.2.3 Sperrmanagement – KEY

vHGS als KOSE		**VU-HGS als KVP oder DL**
TXAS auswerten und TXSLK zurückliefern	<<TXAS << >> TXSLK >> synchron	Abruf der Sperrliste KEY

3.2.4 Sperrmanagement – SAM, ORG

vHGS als KOSE		**VU-HGS als KVP oder DL**
TXAS auswerten und TXSLOS zurückliefern	<<TXAS << >> TXSLOS >> asynchron	Abruf der Sperrliste ORG-SAM
	<< TXSNAWA << asynchron	APP-Sperrnachweis aus SAM-Sperre oder ORG-Sperre einreichen
	<< TXSNAWB << asynchron	BER-Sperrnachweis aus SAM-Sperre oder ORG-Sperre einreichen.
vHGS als AH-Stellvertreter		**VU-HGS als KVP**
APP-Sperrnachweise aus SAM bzw. ORG-Sperren an den KVP der NmApplikation weitergeben.	>> TXSNAWA >> asynchron	
vHGS als PV		**VU-HGS als KVP**
BER-Sperrnachweise aus SAM bzw. ORG-Sperren an den KVP der Berechtigung weitergeben.	>> TXSNAWB >> asynchron	

3.2.5 Aktionsmanagement (RMV-EFS)

vHGS als PV (ALISE)		**VU-HGS als KVP**
	<< TXAAUFBER<< << TXRAUFBER<< << TXEAUFBER<< asynchron	Aktionsaufträge des VU als beauftragender KVP: Berechtigung-Ausgabe, Berechtigung-Rücknahme, Berechtigung-Entsperrung
	<< TXAFREIBER << asynchron	Aktionsfreigabeauftrag des VU als beauftragender KVP
Aktionsfreigabemitteilung des ALISE an beauftragenden KVP	>> TXAFREIMITBER >> asynchron	
	<< TXAS << >>TXAML >> synchron	Aktionsliste herunterladen
	<< TXABER << << TXRBER << << TXSNAWB << asynchron	Als ausführender KVP Transaktionsnachweise aus Aktionsausführungen einreichen: Berechtigung-Ausgabe Berechtigung-Rücknahme Berechtigung-Entsperrung

Weiterleitung von Transaktionsnachweisen aus Aktionsausführungen an den beauftragenden KVP	>> TXABER >> >> TXRBER >> >> TXSNAWB >> asynchron	

3.2.6 Quittungsnachrichten TXA, TXB

Die Quittungsnachrichten TXA und TXB sind in den obigen Tabellen nicht dargestellt. Die Quittungsnachrichten sind entsprechend den Vorgaben der KA Spezifikation zu erzeugen und in einem eigenen Kommunikationsvorgang zu senden.

Beispiel: VU-HGS sendet TXSAUFB an vHGS. vHGS quittiert zunächst nur die technisch erfolgreiche Übermittlung (per http-Rückgabewert „OK“). Nach inhaltlicher Prüfung und Verarbeitung im vHGS sendet vHGS ein TXB (bzw. TXA) an das VU-HGS.

3.3 Ergänzende Festlegungen

3.3.1 TX_BASE, Signatur

Es wird der TX_BASE gemäß KA Spezifikationsversion 1.107 verwendet. Die seitdem vorgenommenen Weiterentwicklungen (siehe KA CR 100) werden nicht berücksichtigt. Die Signaturattribute transSignaturTyp, transSignaturZertifikat und transSignatur werden nicht verwendet. Diese Attribute werden nicht gefüllt.

3.3.2 TX_BASE, Adressierung der KA-Nachrichten

In der Schnittstelle werden zur Adressierung die Sender- und Empfängerattribute des TX_BASE verwendet. D.h. an dieser Stelle werden die Org-IDs des RMV sowie der VGF bzw. der HEAG verwendet. Wie in Kap. 0 beschrieben, verwenden die Nutzermedien (KA Nutzermediumapplikation) und eTickets (KA Berechtigung, RMV EFS) als KVP-ID die ID der RMV KVP-Agentur; die Sender- und Empfängerattribute des TX_BASE dienen ausschließlich der Adressierung.

Mit Bezug auf die Bezeichnungen in den Tabellen in Abschnitt 3.2 ergeben sich folgende Adressierungen:

Bezeichnung	**Org-ID**	**Test Org-ID**	**Rollencode**
vHGS als PV	36	32804	3
vHGS als ALISE (PV)	36	32804	3
vHGS als AH-Stellvertreter	36	32804	4
vHGS als KOSE	36	32804	5
VGF VU-HGS als KVP	6084	38852	1
VGF VU-HGS als DL	6084	38852	2
HEAG VU-HGS als KVP	6180	38948	1
HEAG VU-HGS als DL	6180	38948	2

3.3.3 Sperrlisten

Das vHGS stellt alle innerhalb des eTicket RheinMain erforderlichen Sperrlisten bereit. Bis zum Anschluss an das ION enthält die TXSLNM nur Einträge für eTicket RheinMain Nutzermedien, die TXSLK nur Einträge für eTicket RheinMain Schlüssel und die TXSLOS nur Einträge für eTicket RheinMain SAMs und Organisationen.

Die Bereitstellung der Sperrlisten an der Schnittstelle erfolgt immer als Gesamtliste (keine Differenzlisten). Eine Konfiguration des KOSE ist nicht erforderlich (per Definition erhält jeder Nutzer des vHGS KOSE die Berechtigungssperren aller RMV-Produkte).

3.3.4 Defekte Medien

Die Meldung defekter Medien und deren Sperrung ist ein wichtiges Element zum Schutz des Gesamtsystems vor Missbrauch. Da auf die automatisierte Übermittlung von Sperranfragen verzichtet wird, müssen als defekt gemeldete Medien, für die nicht im eigenen System der Sperrauftrag erzeugt werden kann, per E-Mail oder Fax an das zuständige System übermittelt werden, so dass dort der Sperrauftrag eingegeben werden kann.

Dabei dient die übergeordnete fachliche Betriebsführung des vHGS als Klärungsstelle, da sie anhand der in das vHGS importierten Nutzermedienlieferlisten ermitteln kann, ob ein Nutzermedium von der VGF, der HEAG oder einem der vHGS-Mandanten in Umlauf gebracht wurde. Es ergibt sich folgender Prozess:

- Wird bei der VGF ein defektes Nutzermedium registriert, das von der VGF ausgegeben wurde, dann erstellt die VGF einen Sperrauftrag (TXSAUFA).
- Wird bei der VGF ein defektes Nutzermedium registriert, das nicht von der VGF ausgegeben wurde, dann übermittelt die VGF die aufgedruckte Nummer des Nutzermediums per E-Mail oder Fax an die übergeordnete fachliche Betriebsführung des vHGS. Diese ermittelt anhand der Nutzermediennummer, durch wen das als defekt gemeldete Nutzermedium ausgegeben wurde.
  - Falls HEAG: Übermittlung der Nutzermediennummer per E-Mail oder Fax an die HEAG.
  - Falls vHGS-Mandant: Eingabe einer Sperranfrage in das vHGS. Der betroffene Mandant erstellt daraufhin den Sperrauftrag (TXSAUFA).
- Die bei der HEAG anzuwendende Verfahrensweise ist analog zu der bei VGF.
- Wird bei einem der vHGS-Mandanten ein defektes Nutzermedium registriert, das von einem der vHGS-Mandanten ausgegeben wurde, dann wird innerhalb des vHGS eine Sperranfrage und in der Folge ein Sperrauftrag (TXSAUFA) erstellt.
- Wird bei einem der vHGS-Mandanten ein defektes Nutzermedium registriert, das nicht von einem der vHGS-Mandanten ausgegeben wurde, dann übermittelt der Mandant die aufgedruckte Nutzermediennummer per E-Mail oder Fax an die übergeordnete fachliche Betriebsführung des vHGS. Diese ermittelt anhand der Nutzermediennummer, durch wen (VGF oder HEAG) das als defekt gemeldete Nutzermedium ausgegeben wurde und übermittelt die Meldung des defekten Nutzermediums (mit Angabe der aufgedruckten Nutzermediennummer) per E-Mail oder Fax an VGF bzw. HEAG.

Dementsprechend müssen sowohl das vHGS als auch die VU-HGS darauf vorbereitet sein, dass die Nutzermediennummer eines defekten Nutzermediums nicht im eigenen Datenbestand gefunden wird. Idealerweise weist das System in diesem Fall den Mitarbeiter darauf hin, wie der Fall weiter zu verfolgen ist (siehe oben).

3.3.5 Übermittlung TXSNAWA vom AH-KOSE an den KVP

In KA Version 1.106 wurden APP-Sperrnachweise (TXSNAWA), die aus APP-Sperraufträgen resultierten, nach ihrem Eintreffen vom KOSE an den KVP der gesperrten NmApplikation weitergeleitet. In der KA Version 1.107 wurde dies dahingehend geändert, dass die Sperrnachweise abgeholt werden, d.h. das KVPS sendet ein TXAS an den AH-KOSE und erhält daraufhin die TXSNAWA zugesendet. In der KA Version 1.107 wurde kein Listenformat definiert, das analog dem Herunterladen einer Sperrliste als Antwort zurückgegeben werden könnte. Seitens des vHGS wird folgendes Verfahren implementiert:

- Das KVPS sendet die Aufforderung zum Senden (TXAS mit Auftragscode 8).
- Das AH-KOSES sendet die seit der letzten Abholung neu eingetroffenen TXSNAWA einzeln nacheinander an das KVPS.

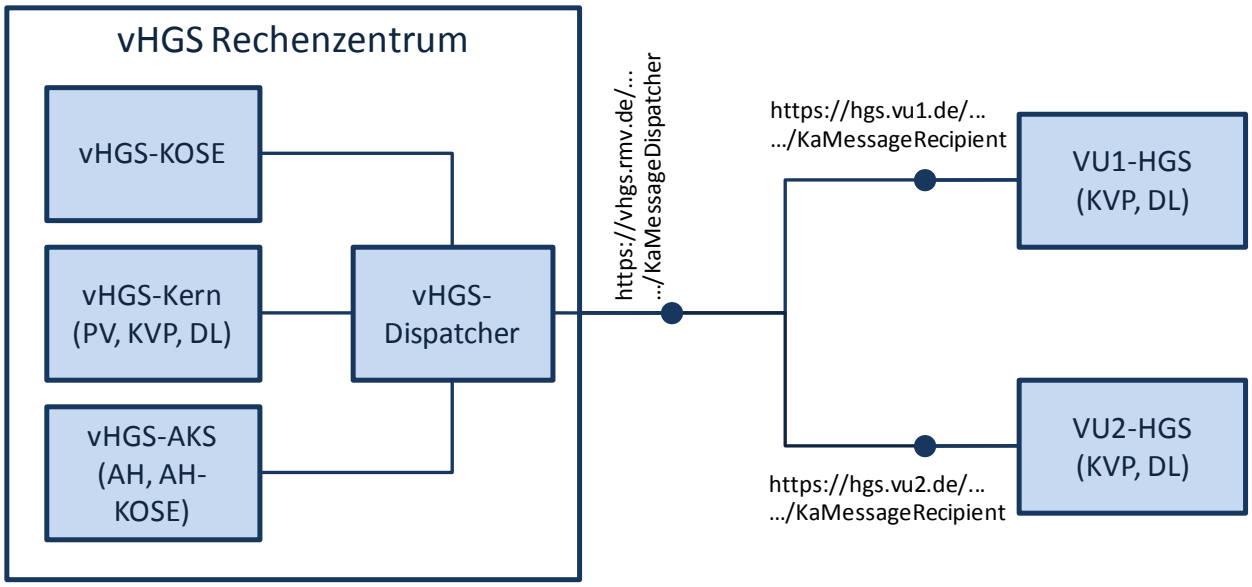
3.4 Technische Festlegungen zur Schnittstelle

Die Schnittstelle zwischen vHGS und den VU-HGS wird durch REST-Webservices implementiert.

Als Kommunikationsprotokoll wird HTTPS eingesetzt.

Das aufrufende System authentisiert sich nach Aufbau der HTTPS-Verbindung mittels Benutzername und Kennwort. Dabei ist der „Benutzer“ das aufrufende System. Der eingesetzte Mechanismus ist die Basic Authentication des HTTP-Protokolls.

Die nachfolgende Abbildung gibt einen Überblick über den Aufbau.



Das vHGS bietet den VU-HGS einen Service „KaMessageDispatcher“ an, über den das System des externen Mandanten KA-Nachrichten einreicht. Der Dispatcher leitet die eingehende Nachricht an das vHGS-Kern-System oder das AH/AH-KOSE-Stellvertreter-System weiter. Die Weiterleitung erfolgt anhand der Empfänger-Attribute (Org-ID und Rolle) im TX_BASE der KA-Nachricht. Der Dispatcher hat dabei keine Pufferfunktion, sondern arbeitet wie eine Telefonvermittlung: der eingehende Aufruf wird gehalten und an das Zielsystem weitergegeben; antwortet das Zielsystem nicht, wird dies dem Aufrufer per http-Fehlercode mitgeteilt.

Die VU-HGS bieten dem vHGS einen Service „KaMessageRecipient“ an, über den das vHGS KA-Nachrichten einreicht.

Die in der Abbildung gezeigten URLs müssen noch im Detail festgelegt werden. Die VU-HGS können die von Ihnen angebotene URL des „KaMessageRecipient“ frei wählen. Im vHGS wird für die KA Org-ID und KA-Rolle(n) jeweils die Ziel-URL des jeweiligen VU-HGS konfiguriert.

Das vHGS und die VU-HGS müssen ständig über die Schnittstelle ansprechbar sein. Für den Fall von planmäßigen (Wartungsarbeiten) oder außerplanmäßigen Zeiten der Nichtverfügbarkeit eines Systems, ist in allen Systemen eine Fehlerbehandlung zu implementieren, die nach einem gescheiterten Verbindungsversuch erneut versucht, die Verbindung aufzubauen. Die erste Wiederholung darf und soll unverzüglich (innerhalb einer Minute) erfolgen. Für alle weiteren Versuche ist ein größerer Zeitabstand zu wählen. Als Empfehlung für sinnvolle Zeitabstände werden dabei die entsprechenden Regelungen aus den Spezifikationen des KA-ION angesehen.

Sofern eines der Systeme einen Stapel von Nachrichten (z.B. weil es aufgrund einer Nichtverfügbakeit des Systems einen Rückstau gegeben hat) an ein anderes System zu versenden hat, wird es die Nachrichten des Stapels nacheinander versenden.

Der HTTPS-Aufruf erfolgt immer mit dem HTTP-Verb POST und die KA-Nachricht wird als Parameter vom Typ text/xml übergeben.

Als Rückgabewert wird entweder einer der HTTP-Standardrückgabewerte geliefert (z.B. 200 „OK“) oder eine KA XML-Datenstruktur (siehe nachfolgende Beschreibung).

In Bezug auf die Rückgabewerte der Schnittstellenaufrufe und damit letztlich den Kommunikationsablauf zur Abwicklung eines Anwendungsfalls wird in Anlehnung an die ION-Spezifikation zwischen fachlich synchroner und fachlich asynchroner KA-Kommunikation unterschieden:

- Fachlich asynchroner KA-Datenaustausch: Übermittlung eines Transaktionsdatensatzes, der vom Empfänger mit TXA/TXB fachlich quittiert wird.

  Beispiel: Übermittlung eines Sperrauftrags TXSAUFA an den KOSE.

  Alle Datenflüsse, die gemäß dem asynchronen Muster abgewickelt werden, sind in den Tabellen in Kap. 3.2 mit dem Wort „asynchron“ gekennzeichnet.

- Fachlich synchroner KA-Datenaustausch: Abfrage von Daten.

  Beispiel: Sperrliste TXSLNM herunterladen.

  Alle Datenflüsse, die gemäß dem synchronen Muster abgewickelt werden, sind in den Tabellen in Kap. 3.2 mit dem Wort „synchron“ gekennzeichnet.

Ablauf für fachlich asynchrone KA-Nachrichten vom VU-HGS an das vHGS:

- VU-HGS ruft https://vhgs.rmv.de/.../KaMessageDispatcher auf und übergibt dabei die KA-Nachricht TXyyy. Rückgabewert des Aufrufs ist http OK (oder ggf. ein http-Fehlercode).
- Nach fachlicher Prüfung und Verarbeitung der KA-Nachricht TXyyy im vHGS ruft das vHGS https://hgs.vu.de/.../KaMessageRecipient auf und übergibt dabei TXA bzw. TXB. Rückgabewert des Aufrufs ist http OK (oder ggf. ein http-Fehlercode).

Der Ablauf für fachlich asynchrone KA-Nachrichten vom vHGS an ein VU-HGS ist analog.

Ablauf für fachlich synchrone KA-Nachrichten vom VU-HGS an das vHGS:

- VU-HGS ruft https://vhgs.rmv.de/.../KaMessageDispatcher auf und übergibt dabei die KA-Nachricht TXaaa. Rückgabewert des Aufrufs ist die KA-Datenstruktur (xml) mit den abgefragten Daten (oder ggf. ein http-Fehlercode).

3.5 KA XML-Schema

Als KA XML-Schema wird

- KA_XML-Schema_V1107_K20110801.xsd

verwendet. Soweit in der genannten XSD noch Fehler entdeckt werden, wird eine entsprechend korrigierte Folgeversion eingesetzt.

3.6 Sonderfallbehandlung für externe Mandanten im vHGS

Die Verwendung der KVP-ID der RMV KVP-Agentur durch externe Systeme (ohne Datensynchronisation im Sinne der bidirektionalen Schnittstelle) erfordert im vHGS eine Erweiterung der Datenverarbeitungsregeln. Bislang gab es externe KVP/DL (die ihre eigene Org-ID verwenden und gemäß den Regeln der KA mit dem PV, KOSE, KVP, DL im vHGS kommunizieren) und vHGS-Mandanten (die als Mitglieder der eTicket RheinMain KVP-Agentur/ DL-Agentur die Org ID des RMV verwenden). Durch die Anbindung der VGF und der HEAG als externe Mandanten über die in den vorangegangenen Abschnitten beschriebene Schnittstelle, müssen die nachfolgend beschriebenen Sonderfallbehandlungen implementiert werden.

Die im vHGS erforderlichen Sonderfallbehandlungen für externe Mandanten (VGF, HEAG) bauen darauf auf, dass im vHGS eine Liste mit den Org-IDs der externen Mandanten eingerichtet wird. Den Org-IDs der externen Mandanten werden Nummernkreise für Nutzermedien (Nutzermedium-ID, NmAppinstanz-ID) und Berechtigungen (Berechtigung-ID) zugewiesen. Diese Nummernkreise sind in allen beteiligten Systemen (VGF, HEAG, vHGS) bei der Ausgabe von Nutzermedien und Berechtigungen zwingend zu beachten.

Sonderfallbehandlung für von VGF bzw. HEAG ausgegebene Nutzermedien und Berechtigungen, wenn diese am Kartenleser der pVks eingelesen werden: Das vHGS muss erkennen, dass diese trotz RMV KVP Agentur ID als „extern verwaltete“ Nutzermedien bzw. Berechtigungen nicht im Service durch Dritte bearbeitet werden dürfen.

Sonderfallbehandlung bei der Weiterleitung von Sperrnachweisen: Das vHGS muss erkennen, dass diese Nachweise obwohl sie sich auf Berechtigungen bzw. NmApplikationen beziehen, die die RMV KVP-Agentur ID als KVP-ID verwenden, an ein externes System (VU-HGS der VGF bzw. HEAG) weiter zu leiten sind.

Sonderfallbehandlung bei der Weiterleitung von Transaktionsnachweisen aus Aktionsausführung: Das vHGS muss erkennen, dass diese Nachweise obwohl sie sich auf Berechtigungen beziehen, die die RMV KVP-Agentur ID als KVP-ID verwenden, an ein externes System (VU-HGS der VGF bzw. HEAG) weiter zu leiten sind.

Für das Senden und Empfangen von KA-Transaktionsdatensätzen, muss das vHGS damit umgehen können, dass Sender- bzw. Empfänger-Org-ID im TX BASE und Org-ID des Transaktionsgegenstands voneinander abweichen, wo sie gemäß KA-Spezifikation übereinstimmen würden (z.B. KVP-ID in der Berechtigung-ID eines TXSAUFB stimmt mit Org-ID des Senders überein).

Sonderfallbehandlung bei der Erfassung defekter Medien, insbesondere auch Verarbeitung der TXKNAWDM aus den Kontrollgeräten: Das vHGS muss erkennen, wenn im vHGS eingegangene Kontrollnachweise TXKNAWDM Nutzermedien betreffen, die von VGF oder HEAG ausgegeben wurden. Die Daten sind in einer gesonderten Liste auszuweisen, so dass sie per Telefon/Fax/E-Mail an VGF bzw. HEAG übermittelt werden können, damit dort entsprechende Sperraufträge eingegeben werden können. Umgekehrt müssen auch VGF und HEAG entsprechende Listen an die üfB übermitteln.

Die Betrugsanalyse (Transaktionsprüfungen des PV gemäß KA Verfahrensanweisung sowie weitere automatisierte Datenauswertungen im vHGS zur Identifizierung von potentiellen Betrugsversuchen) muss dahingehend geändert werden, dass im vHGS eingegangene Kontrollnachweise (TXEBER), die sich auf Berechtigungen beziehen, die von VGF bzw. HEAG ausgegeben wurden, nicht darauf geprüft werden, ob für die entsprechende Berechtigung der

Ausgabenachweis vorliegt. Weiterhin kann für alle Berechtigungen nicht mehr geprüft, werden, ob die Transaktionen (berLogSeqNummer, berSyncronNummer)) lückenlos vorliegen.

4 Bewertung im Hinblick auf das Sicherheitsmanagement

Das KA-Sicherheitssystem besteht aus zwei Elementen:

1. Ein auf anerkannte kryptografische Verfahren gestützter Schutzmechanismus, der die Echtheit und Unverfälschtheit der Transaktionsdaten gewährleisten soll.
2. Eine Überwachung, ob der Schutzmechanismus intakt ist.

Das in diesem Dokument beschriebene Konzept zur Schnittstelle zwischen VGF/HEAG und dem vHGS schwächt die kryptografischen Verfahren nicht. Einschränkungen gibt es jedoch im Bereich der Überwachung.

Die Einschränkungen betreffen die folgenden von der KA vorgesehenen Prüfungen des RMV als PV für eTicket RheinMain Berechtigungen (RMV-EFS):

- *Ausgabetransaktion TXABER liegt vor*

  Dies kann für Berechtigungen, die von VGF bzw. HEAG ausgegeben wurden, nicht geprüft werden.

- *Lückenlosigkeit der berLogSeqNummer*

  Dies kann für alle Berechtigungen nicht geprüft werden. Es sind jedoch damit verwandte Prüfungen (doppelt auftretende berLogSeqNummer, auffällig große Lücken) anhand der Daten möglich, die dem PV von den vHGS-Mandanten geliefert werden.

- *Lückenlosigkeit der berSynchronNummer*

  Dies kann für Berechtigungen, die von VGF bzw. HEAG ausgegeben wurden, nicht geprüft werden.

Die oben genannten Einschränkungen sind für eine Übergangszeit vertretbar, insbesondere wenn VGF und HEAG in ihren Systemen für die von Ihnen ausgegebenen Berechtigungen die Eigenschaften *„Ausgabetransaktion TXABER liegt vor“* und *„Lückenlosigkeit der berSynchronNummer“* überwachen.

Der am leichtesten realisierbare Betrugsversuch durch Nutzer ist die Verwendung defekter Nutzermedien sowie die „Duplizierung“ von Nutzermedien durch Ersatznutzermedien aus einer Verlust-/Defektmeldung. Das Erfassen defekter Nutzermedien bei den Kontrollen und das anschließende Erstellen von Sperraufträgen sowie die Nachprüfung (EBE-Androhung), ob das defekte Nutzermedium eine gültige Fahrberechtigung enthielt, sollte daher möglichst konsequent umgesetzt werden. Die durch den gewählten Zuschnitt der Schnittstelle zwischen vHGS und den Systemen der VGF und der HEAG bestehenden Einschränkungen können durch organisatorische Maßnahmen (Erstellung und Austausch von Listen, telefonische Klärung von Verdachtsfällen) ausgeglichen werden.

RHEIN-MAIN-VERKEHRSVERBUND

Teilnehmer am vHGS

Liste mit allen Teilnehmern am vHGS
nach Aufgabenbereich

Anlage 7 zum vHGS-Vertrag

Thema:	Teilnehmer am vHGS
Dateiname:	Anlage7_Teilnehmer vHGS
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	0.98
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
0.9	RMV	08.12.2011	Die Liste der Teilnehmer enthält den Kenntnisstand zum 08.12.2011. Die abschließende Version 1.0 wird nach Abschluss der Vertragsunterzeichnungen nachgereicht.
0.91	RMV	15.04.2014	Die Liste der Teilnehmer enthält den Kenntnisstand zum 15.04.2014. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.92	RMV	05.10.2015	Die Liste der Teilnehmer enthält den Kenntnisstand zum 05.10.2015. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.93	RMV	20.02.2017	Die Liste der Teilnehmer enthält den Kenntnisstand zum 20.02.2017. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.94	RMV	18.08.2017	Die Liste der Teilnehmer enthält den Kenntnisstand zum 18.08.2017. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.95	RMV	07.12.2017	Die Liste der Teilnehmer enthält den Kenntnisstand zum 07.12.2017. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.96	RMV	09.02.2018	Die Liste der Teilnehmer enthält den Kenntnisstand zum 09.02.2018. Die abschließende Version wird nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.97	RMV	16.04.2018	Die Liste der Teilnehmer enthält den Kenntnisstand zum 16.04.2018. Die abschließende Version wird

			nach Abschluss aller Vertragsunterzeichnungen nachgereicht. Neu hinzugekommene Mandanten sind jeweils farbig hinterlegt.
0.98	RMV	20.02.2019	Erweiterung der Tabelle um den Aufgabenbereich „Vertrieb JobTicket ohne Service durch Dritte“

Die Teilnehmer am vHGS nehmen folgende Aufgabenbereiche wahr:

Teilnehmer	Aufgabenbereich					Vertragsabschluss
	Online vHGS*	Vertrieb JobTi-Ticket°	Offline vHGS	Ticket Shop	Kontrolle	
ALV Marburg/Oberhessen GmbH & Co. oHG Ernst-Giller-Straße 7 35039 Marburg	x			x	x	02.04.2012 (letztes Datum Teilnahmevertrag)
Andreas Bonifer Spedition und Verkehrs-unternehmen GmbH & Co KG Seligenstädter Str. 127 - 135 63073 Offenbach					x	27.02.2012 (letztes Datum Teilnahmevertrag)
Autobus Sippel GmbH Hessenstraße 16 65719 Hofheim am Taunus					x	08.12.2014 (letztes Datum vHGS-Vertrag)
B.u.S. Linienverkehr Bender Reisen Am Hofacker 6 35630 Ehringshausen					x	10.11.2016 (letztes Datum vHGS Vertrag)
Balser Reisen GmbH An der Saline 16 63654 Büdingen					x	29.04.2013 (letztes Datum Teilnahmevertrag)
Becker & Sohn GmbH & Co. KG Am Bewegungsbad 1 - 5 35080 Bad Endbach	x				x	27.02.2012 (letztes Datum Teilnahmevertrag)
Busverkehr Wissmüller GmbH Neutorstrasse 10 64720 Michelstadt					x	
DB Regio AG Region Hessen Mannheimer Straße 81 60327 Frankfurt am Main	x			x	x	09.12.2011 (letztes Datum Teilnahmevertrag)
DeinBus Verkehrs-GmbH Georg-Ohm-Straße 1 74235 Erlenbach					x	23.10.2017 (letztes Datum vHGS Vertrag)
~~DNSW Dieselnetz Südwest GmbH~~ Vlexx GmbH-Metronom Adam-Karrillon-Str. 13 55118 Mainz					x	23.05.2014 (letztes Datum vHGS Vertrag)
~~Dieter Schwalb Reisen e.K.~~ Schwalb Verkehrsbetrieb KG Reiskirchener Str. 21 35418 Buseck - Beuern					x	16.08.2017 (letztes Datum vHGS Vertrag)
Energie Waldeck-	x		x	x	x	06.04.2017 (letz-

Frankenberg GmbH (EWF) Arolser Landstraße 27 34497 Korbach						tes Datum vHGS Vertrag)
Erletz Reisen GmbH Schiffenweg 2 35460 Staufenberg					x	16.08.2017 (letztes Datum Teilnahmevertrag)
ESWE Verkehrsgesellschaft mbH Gartenfeldstraße 18 65189 Wiesbaden					x	
BRH viabus GmbH (First Group Rhein-Neckar GmbH) Ostring 20 63533 Mainhausen-Zellhausen					x	02.04.2012 (letztes Datum Teilnahmevertrag)
Gebrüder Schermuly GmbH & Co KG Hohe Straße 21 35794 Mengerskirchen					x	22.04.2014 (Datum beider Verträge identisch)
Georg Becker GmbH & Co. KG Flachsbachstr. 40 - 42 63225 Langen					x	16.08.2013 (letztes Datum Teilnahmevertrag)
Hanauer Straßenbahn GmbH Daimlerstr. 5 63450 Hanau	x			x	x	18.12.2014 (letztes Datum vHGS-Vertrag)
~~HAV Verkehrsbetriebsgesellschaft & Co. KG Bismarckstraße 112-114 64293 Darmstadt~~					~~x~~	~~27.02.2012 (letztes Datum Teilnahmevertrag)~~
HEAG mobiBus GmbH & Co. KG Klappacher Straße 172 64285 Darmstadt					x	
HEAG mobilo GmbH Klappacher Straße 172 64285 Darmstadt			x			
Hessische Landesbahn GmbH Am Hauptbahnhof 18 60329 Frankfurt am Main					x	
Heuser Omnibusunternehmen GmbH & Co.KG Kinzigstraße 10 63505 Langenselbold	x			x	x	20.11.2012 (letztes Datum vHGS Vertrag)
HLB Basis AG Am Hauptbahnhof 18 60329 Frankfurt am Main	x			x	x	15.01.2015 (letztes Datum vHGS Vertrag)
Kahlgrund-Verkehrs-Gesellschaft mbH Am Bahnhof 12 63825 Schöllkrippen					x	03.03.2017 (letztes Datum vHGS Vertrag)

Karl Hasenauer GmbH & Co. KG Vogelsbergstraße 192 63679 Schotten					x	22.12.2016 (letztes Datum Teilnahmevertrag)
Kasseler Verkehrs-Gesellschaft AG Königstor 3-13 34117 Kassel					x	03.07.2017 (letztes Datum vHGS Vertrag)
Kraftverkehr Keller & Co. KG Bornweg 18 35638 Leun/Biskirchen					x	27.10.2014 (Datum der Verträge identisch)
Kraftverkehr Lauterbach GmbH & Co. KG Fuldaer Str. 29 36341 Lauterbach					x	08.02.2012 (letztes Datum vHGS Vertrag)
Kreisverkehrsgesellschaft Main-Kinzig mbH Nürnberger Str. 41 63450 Hanau	x			x	x	29.04.2013 (letztes Datum Teilnahmevertrag)
Kreis-Verkehrs-Gesellschaft Offenbach mbH Masayaplatz 1 63128 Dietzenbach	x			x	x	25.01.2012 (letztes Datum vHGS Vertrag)
LNVG Groß-Gerau Lokale Nahverkehrsgesellschaft mbH des Kreises Groß-Gerau Jahnstraße 1 64521 Groß-Gerau	x			x	x	06.05.2013 (letztes Datum vHGS Vertrag)
Lokale Nahverkehrsgesellschaft Fulda mbH Zieherser Weg 2 36037 Fulda	x			x		03.02.2012 (letztes Datum Teilnahmevertrag)
Magistrat der Stadt Bad Homburg v.d.Höhe Produktbereich ÖPNV Rathausplatz 1 61348 Bad Homburg v.d.Höhe	x				x	24.04.2014 (letztes Datum vHGS Vertrag)
Mainzer Verkehrsgesellschaft mbH (MVG) Mozartstraße 8 55118 Mainz	x				x	23.07.2014 (letztes Datum vHGS Vertrag)
Main-Taunus-Verkehrsgesellschaft mbH (MTV) Am Kreishaus 1-5 65719 Hofheim a. Taunus	x			x	x	07.07.2014 (letztes Datum vHGS Vertrag)
Medenbach Traffic GmbH Pfingstborn 3 35781 Weilburg					x	23.05.2013 (letztes Datum Teilnahmevertrag)
MIT.BUS GmbH					x	09.02.2018 (letz-

Lahnstraße 31 35398 Gießen						tes Datum vHGS Vertrag)
Nahverkehr Schwalm-Eder GmbH (NSE) Parkstraße 6 34576 Homberg (Efze)	x		x	x	x	06.04.2017 (letztes Datum vHGS Vertrag)
Nassauische Verkehrs-Gesellschaft mbH Im Gewerbegebiet Heide 56357 Bogel					x	30.11.2016 (letztes Datum Teilnahmevertrag)
Offenbacher Verkehrsbetriebe GmbH (OVB) Hebestraße 14 63065 Offenbach	x			x	x	16.08.2013 (letztes Datum Teilnahmevertrag)
Omnibusbetrieb Eberwein Berlinerstrasse 19 b 61184 Karben					x	29.04.2013 (letztes Datum Teilnahmevertrag)
Omnibusbetrieb Winzenhöler GmbH & Co. KG Waldstraße 84 64846 Groß-Zimmern					x	02.04.2012 (letztes Datum Teilnahmevertrag)
Omnibusunternehmen Karl-Heinz Klüh Hintersteinauer Str. 6 36381 Schlüchtern					x	16.01.2013 (letztes Datum vHGS Vertrag)
Odenwald -Regional-Gesellschaft mbH (OREG) Marktplatz 1 64711 Erbach	x			x	x	03.02.2012 (letztes Datum Teilnahmevertrag)
~~ORN Omnibusverkehr Rhein-Nahe GmbH~~ DB Regio Bus Südwest GmbH Erthalstraße 1 55118 Mainz					x	08.12.2016 (letztes Datum vHGS Vertrag)
Philippi Nahverkehr GmbH & Co. KG Alsfelder Straße 34 35325 Mücke/ Groß-Eichen					x	27.02.2012 (letztes Datum Teilnahmevertrag)
Racktours GmbH & Co.KG Auf dem Hessel 8 63526 Erlensee					x	06.05.2013 (letztes Datum vHGS Vertrag)
Regionaler Nahverkehrsverband Marburg-Biedenkopf (RNV) Im Lichtenholz 60 35043 Marburg	x				(x)	06.05.2014 (letztes Datum vHGS Vertrag)
~~Regionalverkehr Kurhessen GmbH~~ ~~Bosestraße 3~~ ~~34121 Kassel~~					~~x~~	
Regionalverkehr Main-Kinzig GmbH					x	05.06.2013 (letztes Datum Teil-

Barbarossastr. 28 - 30 63571 Gelnhausen						nahmevertrag)
Regionalverkehrsdienst Gründau Elke Laubach e.K. Brauhausweg 9 63584 Gründau	x			x	x	20.11.2012 (letztes Datum vHGS Vertrag)
Reiseservice Frieda Gass Alpenstraße 6 36119 Neuhof-Hauswurz					x	27.03.2017 (letztes Datum Teilnahmevertrag)
RTV Rheingau-Taunus-Verkehrsgesellschaft mbH Heimbacher Straße 7 65307 Bad Schwalbach	x			x	x	03.12.2012 (letztes Datum Teilnahmeverrag)
~~Schreiber Reisen GmbH Distelbachstr. 12 36396 Steinau a. d. Straße~~					~~x~~	
Spahn + Roth Industriering 2 64850 Schaafheim					x	03.02.2012 (letztes Datum Teilnahmevertrag)
Stadtverkehr Maintal GmbH Berliner Str. 31 63477 Maintal	x				x	05.04.2013 (letztes Datum Teilnahmevertrag)
Stadtwerke Bad Nauheim GmbH Hohe Straße 14-18 61231 Bad Nauheim					x	
Stadtwerke Bad Vilbel GmbH Theodor-Heuss-Strasse 51 61118 Bad Vilbel					x	
Stadtwerke Dietzenbach GmbH Thomas-Mann-Ring 2 - 4 63128 Dietzenbach			x		x	
Stadtwerke Friedrichsdorf Hugenottenstr. 55 61381 Friedrichsdorf	x				x	20.01.2017 (letztes Datum vHGS Vertrag)
Stadtwerke Gießen AG Lahnstraße 31 35398 Gießen	x			x	x	17.01.2018 (letztes Datum vHGS Vertrag)
Stadtwerke Langen GmbH Weserstraße 14 63225 Langen			x		x	
Stadtwerke Marburg GmbH Am Krekel 55 35039 Marburg	x			x	x	27.02.2012 (letztes Datum Teilnahmevertrag)
Stadtwerke Mühlheim am Main GmbH Dietesheimer Straße 70 63165 Mühlheim am Main					x	
Stadtwerke Neu-Isenburg GmbH			x		x	

Schleussnerstraße 62 63263 Neu-Isenburg						
Stadtwerke Oberursel (Taunus) GmbH Oberurseler Straße 55 - 57 61440 Oberursel (Taunus)	x				x	03.02.2012 (letztes Datum Teilnahmevertrag)
Stadtwerke Rodgau Friedberger Straße 37 63110 Rodgau			x		x	
Stadtwerke Rüsselsheim GmbH Walter-Flex-Straße 74 65428 Rüsselsheim	x				x	07.07.2014 (letztes Datum vHGS-Vertrag)
Stroh Busverkehrs GmbH Goethestraße 1-5 63674 Altenstadt	x				x	29.07.2013 (letztes Datum vHGS Vertrag)
traffiQ Lokale Nahverkehrsgesellschaft Frankfurt am Main mbH Stiftstraße 9-17 60313 Frankfurt am Main					x	24.06.2014 (letztes Datum vHGS Vertrag)
Transdev Rhein-Main GmbH Flinschstraße 22 60388 Frankfurt am Main					x	12.12.2016 (letztes Datum Teilnahmevertrag)
~~ÜWAG Überlandwerk Fulda Aktiengesellschaft~~ RhönEnergie Fulda GmbH Bahnhofstraße 2 36037 Fulda	x			x	x	07.05.2012 (letztes Datum Teilnahmevertrag)
~~ÜWAG Bus GmbH~~ RhönEnergie Bus GmbH Heinrichstraße 17/19 36037 Fulda	x				x	07.05.2012 (letztes Datum Teilnahmevertrag)
~~VLD Verkehrsbetrieb Lahn-Dill GmbH Brunnenstr. 11 65551 Limburg - Lindenholzhausen~~					x	
Verkehrsbetriebe Stadtwerke Dreieich Eisenbahnstraße 140 63303 Dreieich			x		x	
Verkehrsbetrieb Weber GmbH Jahnstraße 1 35444 Biebertal					x	10.11.2016 (letztes Datum vHGS Vertrag)
Verkehrsgesellschaft Gersprenztal mbH Am Pfeiffersteg 4 64385 Reichelsheim	x		x	x	x	10.05.2017 (letztes Datum Teilnahmevertrag)
Verkehrsgesellschaft Lahn-Dill-Weil mbH	x			x		19.11.2012 (letztes Datum Teil-

Karl-Keller-Ring 49 35576 Wetzlar						nahmevertrag)
Stadtwerke Verkehrsgesellschaft Frankfurt am Main mbH (VGF) Kurt-Schumacher-Straße 8 60311 Frankfurt am Main		x				
Verkehrsgesellschaft Region Fulda (VGF) Heinrichstraße 17 36037 Fulda	x				x	2015 (letztes Datum vHGS-Vertrag)
VGO Verkehrsgesellschaft Oberhessen mbH Hanauer Str. 15 61169 Friedberg	x			x	x	03.02.2012 (letztes Datum Teilnahmevertrag)
Verkehrsverband Hochtaunus (VHT) Ludwig-Erhard-Anlage 1-5 61352 Bad Homburg	x			x	x	12.04.2016 (letztes Datum vHGS Vertrag)
VIAS GmbH Gebäude-Nr. 5401 Stroofstr. 27 65933 Frankfurt am Main					x	09.02.2012 (letztes Datum vHGS Vertrag)
~~VM Verkehrsgesellschaft Mittelhessen GmbH Raiffeisenstraße 10 61250 Usingen~~					~~x~~	
Werner Gimmler Wetzlarer Verkehrsbetriebe und Reisebüro GmbH Siegmund-Hiepe-Straße 24 - 26 35578 Wetzlar	x				x	23.11.2017 (letztes Datum vHGS Vertrag)

* inkl. Service durch Dritte
° ohne Service durch Dritte

RHEIN-MAIN-VERKEHRSVERBUND

Glossar vHGS

Glossar zum Vertrag über die
Nutzung, Teilnahme und Zusammenarbeit am verbundweiten mandantenfähigen Hintergrundsystem (vHGS) des eTicket RheinMain (vHGS-Vertrag)

Anlage 8 zum vHGS-Vertrag

Thema:	Glossar vHGS
Dateiname:	Anlage8_Glossar
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	1.3
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Version als Anlage zum vHGS-Vertrag V1.0
1.1	rms	04.10.2018	Aufgabenbereich „Vertrieb von Jobtickets ohne Service durch Dritte“
1.2	RMV	16.10.2018	Aufgabenbereich „Vertrieb JobTicket ohne Service durch Dritte“
1.3	RMV	20.02.2019	Ergänzung um neue Begriffe, deren Kürzel und Bedeutung (DSGVO, VDL)

AH	Applikationsherausgeber Der AH ist der Herausgeber der KA ÖPV-Applikation für das Nutzermedium. Der AH verwaltet und vergibt alle für das KA-Sicherheitssystem relevanten Schlüssel. Der AH registriert alle teilnehmenden Organisationen und vergibt Identifikatoren an diese. Der AH zertifiziert Komponenten und sorgt für die Weiterentwicklung der Spezifikationen. Die Rolle des AH wird durch die VDV-KA KG wahrgenommen.
AHS	Applikationsherausgebersystem
Aktionsliste	Vom ALISE erstellte KVP-spezifische Liste der Aktionsaufträge.
Aktionsmanagement	Verfahren bei dem bestimmte Vorgänge als sogenannte Aktionen an einem beliebigen Vertriebsterminal im System beauftragt werden und später, wenn das relevante Nutzermedium mit einem zur Ausführung von Aktionen vorgesehenen Terminal in Kontakt kommt, automatisch ausgeführt werden. Im eTicket RheinMain erfolgt z.B. der Verkauf von Berechtigungen im TicketShop über das Aktionsmanagement. Über das Aktionsmanagement ist auch eine Rückgabe, Änderung oder Sperrung von Berechtigungen und die Sperrung der Applikation auf einem Nutzermedium möglich.
ALISE	Aktionslistenservice. Der ALISE ist eine Spezialisierung der Rolle PV, die bei Anwendung des Aktionsmanagements die entsprechende Funktionalität eines Aktionslistenservice-Systems (ALISES) in ihrem PVS vorzuhalten hat.
APP	Siehe Applikation
Appinstanz-ID	Im gesamten Geltungsbereich der Kernapplikation eindeutige Kennzeichnung einer an einen Kunden ausgegebenen ÖPV-Applikation (siehe KA BOM-SPEC, V1.107).
Applikation	Daten, Kommandos, Abläufe, Zustände, Mechanismen, Algorithmen und Programmcode innerhalb einer Chipkarte, um diese im Rahmen eines bestimmten Systems (hier des eTicket RheinMain bzw. des (((eTicket Deutschland) zu betreiben. Zu den Mechanismen zählen die Einbindung in die Sicherheitsarchitektur des jeweiligen Gesamtsystems sowie die Übertragungsprotokolle zu den Back End Systemen.
Aufgabenmanagement	Aufgabenmanagement des vHGS; Über das Aufgabenmanagement werden dem zuständigen Mandanten Aufgaben, die eigene Kunden des Mandanten betreffen und von anderen Mandanten im Service durch Dritte oder vom Kunden über die Onlineplattform „mein RMV“ ausgelöst wurden, zur Bearbeitung bereitgestellt.

Ausbauvariante	Die VDV-KA sieht folgende Ausbauvarianten vor: (((eBezahlen (Variante 1), (((eFahrschein (Variante 2) und Automatisierte Fahrpreisermittlung (Variante 3). Nähere Erläuterungen finden sich in Abschnitt 3 des Dokuments KA KUSCH-SPEC (siehe auch Kapitel 3, Ziffer 10 des (((eTicket-Regelwerks) der VDV-KA KG.
Ausbauvariante 2a	Migrationsschritt auf dem Weg zu einer vollständigen Realisierung der Ausbauvariante 2. Ausbauvariante 2a beschränkt sich auf „Produkte für Stammkunden“ (z.B. elektronische Abonnement-Zeitfahrausweise, Jahreskarten)
Authentisierung	Nachweis der eigenen Identität. Möglichkeiten der Authentisierung sind: - Nachweis der Kenntnis einer Information, zum Beispiel eines Passwortes, - Verwendung eines Besitztums, zum Beispiel eines Schlüssels oder - Gegenwart des Benutzers selbst und Nachweis der Identität zum Beispiel in Form eines biometrischen Merkmals.
Automatisierte Fahrberechtigung (AFB)	Berechtigung zur Inanspruchnahme von Beförderungsleistungen eines DL mit Automatisierter Fahrpreisermittlung unter Nutzung einer (((eBezahlberechtigung
Autorisierung	Zuweisung von Zugriffsrechten auf Daten und Dienste. Entscheidung, welcher Benutzer Zugriff auf welche Funktionen innerhalb einer Anwendung erhält.
Backup	Datensicherung
BDSG	Bundesdatenschutzgesetz
BER	siehe Berechtigung
Berechtigung	Fahrberechtigung, die elektronische Daten zur Inanspruchnahme von Beförderungsleistungen eines DL enthält. Die an die Berechtigung geknüpften Regelungen bzgl. der Inanspruchnahme von Leistungen, Berechnung des Leistungsentgelts und der Bezahlung werden im wesentlichen durch das jeweilige EFM-Produkt festgelegt.
berLogSeqNummer	Transaktionen einer Berechtigung unter Verwendung des Nutzermediums an einem Terminal erhalten jeweils bezogen auf die jeweilige Berechtigung eine fortlaufende Nummer. Diese Sequenznummer liefert einen im Kontext der jeweiligen Berechtigung eindeutigen fachlichen Schlüssel der Transaktion (siehe KA BOM-SPEC, V1.107)

berSynchronNummer	Die Synchronnummer wird bei Statusänderungen der Berechtigung (z.B. Sperr- und Entsperrvorgänge) jeweils um 1 erhöht. Über die Synchronnummer kann ein Offline arbeitendes Terminal erkennen, ob die letzte Statusänderung auf dem Nutzermedium älter oder jünger ist als die letzte dem Terminal von einem Hintergrundsystem übergebene Information (siehe KA BOM-SPEC, V1.107).
Bidirektionale Schnittstelle	Geplante Schnittstelle, über die teilnehmereigene KA-fähige Vertriebs- und Abosysteme mit dem vHGS verbunden werden können. Nach Anbindung an das vHGS können dann auch diese Teilnehmer Leistungen im Rahmen des Service durch Dritte erbringen.
DES	Digital Encryption Standard; Block-Verschlüsselungsverfahren
Dienstleister	Alle Teilnehmer, die Beförderungsleistungen erbringen. Der DL schließt Verträge mit Produktverantwortlichen zur Akzeptanz von Produkten und zur Vergütung der erbrachten Leistungen durch die Produktverantwortlichen.
DL	Abkürzung für Dienstleister
DLS	Dienstleistersystem
DL-Agentur	Das Konzept des eTicket RheinMain sieht vor, dass in der Rolle eines DL gegenüber externen KA-Teilnehmern (außerhalb des RMV-Gebietes) ausschließlich die sogenannte „DL-Agentur in Erscheinung tritt. Die als Mandanten in der Rolle DL in das vHGS eingebundenen Verkehrsunternehmen verwenden die KA Org-ID der gemeinsamen eTicket RheinMain DL-Agentur. Die Zuordnung zu den einzelnen „handelnden DL“ (Verkehrsunternehmen) innerhalb des eTicket RheinMain wird durch das vHGS geleistet.
DMZ	Abkürzung für Demilitarized Zone. Bezeichnet in der EDV ein Computernetzwerk mit sicherheitstechnischer Abschirmung gegen andere damit verbundene Netzwerke.
DSGVO	Datenschutzgrundverordnung
(((eBezahlen	Bargeldloses Bezahlen (z.B. von Papierfahrscheinen) mit einer (((eBezahlberechtigung; Ausbauvariante 1 gemäß VDV-KA
EBE	Erhöhtes Beförderungsentgelt (hier speziell für den Fall, dass auf dem Nutzermedium keine gültige Fahrberechtigung vorhanden ist).
Ende-zu-Ende MAC-Sicherung	Hier: Integritätssicherung der Transaktionsdaten vom Dienstleister bis zu dem für das Nutzermedium zuständigen Kundenvertragspartner und/oder bis zu dem für ein bestimmtes Produkt zuständigen Produktverantwortlichen. Die Ende-zu-Ende-Sicherung wird dadurch erreicht, dass das Nutzermedium einen MAC über die Transaktionsdaten bildet, der vom Dienstleister mit den Transaktionsdaten eingereicht werden muss und der nur von dem entsprechenden Kundenvertragspartner bzw. Produktverantwortlicher geprüft

	werden kann.
ET-Beirat	Fachgremium des RMV zum Thema elektronisches Fahrgeldmanagement.
(((eTicket	Elektronischer Ersatz für Tickets aus Papier. Das (((eTicket ist als Datensatz auf einem Nutzermedium abgespeichert. Eine Ausbauvariante ist der Elektronische Fahrschein (EFS).
EFM	elektronisches Fahrgeldmanagement
EFS	Abkürzung für Elektronischer Fahrschein; Ausbauvariante 2 gemäß VDV-KA. Der elektronische Fahrschein beschreibt einen auf einem Nutzermedium abgelegten kompletten Fahrschein, der mit Ausnahme einer möglichen Entwertung in dieser Form durch einen Fahrgast unmittelbar nutzbar ist, wobei die räumliche und zeitliche Gültigkeit mit Nutzungsbeginn feststeht und im Nachhinein auch nicht mehr verändert wird.
(((eTicket-Deutschland	Markenname der VDV-Kernapplikation als nationaler Standard für elektronisches Fahrgeldmanagement (EFM) in Deutschland Gleichzeitig Bezeichnung der Gesamtheit der (((eTicket-Systeme in Deutschland auf Basis der VDV-Kernapplikation.
eTicket RheinMain	Produktmarke für das elektronische Fahrgeldmanagement (EFM) im RMV
(((eTicket-System	Regional begrenztes, interoperables, elektronisches Fahrgeldmanagementverfahren, das auf der VDV-Kernapplikation beruht und vor Ort in verschiedenen Ausbauvarianten parallel existieren kann; im RMV als eTicket RheinMain bezeichnet.
(((eTicket-Teilnahmevertrag	Vertrag über die Teilnahme am (((eTicket-Deutschland
Externer Mandant	Das Konzept „Externer Mandant“ ist eine Übergangslösung für einen eingeschränkten Datenaustausch zwischen dem vHGS und Teilnehmern mit eigenen KA-fähigen Vertriebs- und Abosystemen. Der Datenaustausch ist auf die für das Sperrmanagement und das Aktionsmanagement zwingend erforderlichen Daten beschränkt. Eine Einbindung in das verbundweite Servicekonzept (Service durch Dritte) ist damit nicht möglich. Diese Übergangslösung wird bis zur Inbetriebnahme der bidirektionalen Schnittstelle benötigt.
FTPS	Verschlüsseltes Dateiübertragungsverfahren auf Basis des File Transfer Protocols (Netzwerkprotokoll zur Übertragung von Dateien über IP-Netzwerke).
HDSG	Hessisches Datenschutzgesetz
HGS	Abkürzung für Hintergrundsystem
Hintergrundsystem	Alle Computersysteme eines (((eTicket-Systems, welche die (((eTicket-Daten der Terminals verwalten und verarbeiten.
HTTPS	HyperText Transfer Protocol Secure: Kommunikationsprotokoll zur abhörsicheren Übertragung von Daten im Internet.

ID	Identifikator: Merkmal zur eindeutigen Identifizierung eines Objektes.
Interoperabilität	Fähigkeit des (((eTicket-Deutschland zur deutschlandweiten Nutzung eines NM´s für die Inanspruchnahme von ÖPV-Leistungen unter Einsatz der (((eBezahlberechtigungen, soweit die entsprechenden (((eTicket-Produkte im Bereich des jeweils regional zuständigen Teilnehmers bzw. des für diesen Bereich zuständigen PV angeboten werden. Wird in Übergangsphasen schrittweise über Migrationsszenarien verwirklicht.
ION	Interoperabilitätsnetzwerk gemäß VDV Kernapplikation
KA	VDV Kernapplikation
KA CR	Change Request zur KA
KA KG	siehe: VDV-KA KG
KA-Nachricht	Siehe TX…
KA XML-Schema	Siehe auch XML-Schema. Das XML-Schema für die VDV-Kernapplikation, Version 1.107 findet sich im Dokument KA_XML-Schema_V1107_K20110801.xsd
KEY	Elektronischer Schlüssel zur Verschlüsselung von Datensätzen
Kontrolle	Aufgabenbereich im vHGS. Im Aufgabenbereich Kontrolle führen die Teilnehmer am vHGS Kontrolltätigkeiten (dh. Kontrollen der Fahrberechtigungen auf den Nutzermedien) durch.
Kontrollnachweis	Nachweis (in Form eines Datensatzes), der aufgrund der Kontrolltätigkeit entsteht.
Kontrollservice	Sperrlistenmanagement (siehe auch Kapitel 5 des (((eTicket-Regelwerks der VDV-KA KG). Der Kontrollservice nimmt sowohl Sperraufträge vom AH zu Organisations-, SAM und Schlüssel-(Key-) Sperren als auch Sperraufträge von KVP zu Applikations- und Berechtigungs-Sperren entgegen. Er generiert aus Sperr- und Entsperraufträgen sowie den Sperrnachweisen die jeweils aktuellen Sperrlisten und stellt diese zur Abholung durch die KVP, DL sowie AH und PV bereit. Für das eTicket RheinMain wird zunächst ein RMV-weites Sperrlistenmanagement etabliert. Der Anschluss an den im Aufbau befindlichen deutschlandweiten Kontrollservice ist für einen späteren Zeitpunkt vorgesehen.
KOSE	Abkürzung für Kontrollservice (Sperrlistenmanagement)
KOSES	Kontrollservicesystem
Kryptogramm	Mit Hilfe eines kryptografischen Verfahrens verschlüsselte Information

Kryptografie	Schutzmechanismus, der die Echtheit und Unverfälschtheit von Daten (hier speziell der KA-Transaktionsdaten) gewährleisten soll
Kunde	Jeder, der einen Kundenvertrag mit einem KVP abgeschlossen hat
Kundenvertrag	Vertrag zwischen einem KVP und dem Kunden, der einzelne oder alle nachfolgend genannten Leistungen im Rahmen des (((eTicket-Deutschland zum Gegenstand hat: - Ausgabe der VDV-Kernapplikation (ggf. zusammen mit der Aushändigung eines NM) - Nutzung einer (((eBezahlberechtigung
Kundenvertragspartner	Alle Teilnehmer, die im eigenen Namen mit ihren Kunden Kundenverträge abschließen und/oder EFS-Vertriebsstelle sind. Der KVP gibt an den Kunden eine Berechtigung aus und nimmt dafür vom Kunden ein Entgelt entgegen.
Kryptographische Verfahren	Verfahren zur Verschlüsselung von Daten. Die Daten sind erst nach Entschlüsselung mittels eines geeigneten Schlüssels im Klartext lesbar.
KVP	Abkürzung für Kundenvertragspartner
KVP-Agentur	Das Konzept des eTicket RheinMain sieht vor, dass in der Rolle eines KVP gegenüber externen KA-Teilnehmern (außerhalb des RMV-Gebietes) ausschließlich die sogenannte „KVP-Agentur“ in Erscheinung tritt. Die als Mandanten in der Rolle KVP in das vHGS eingebundenen Verkehrsunternehmen verwenden die KA Org-ID der gemeinsamen eTicket RheinMain KVP-Agentur. Die Zuordnung zu den einzelnen „handelnden KVP“ (Teilnehmer) innerhalb des eTicket RheinMain wird durch das vHGS geleistet.
KVPS	Kundenvertragspartnersystem
LNO	Lokale Nahverkehrsorganisation
Logging	Protokollieren eines Programmablaufes
MAC	Message Authentication Code; besteht aus Kontrolldaten zum Nachweis, dass eine Nachricht nicht zufällig oder durch Dritte verändert wurde.
Mandant	Der Begriff Mandant wird synonym für Teilnehmer am vHGS genutzt.

mandantenfähig	Ein System ist mandantenfähig, wenn jeder Mandant nur Zugriff auf seine Daten, nicht aber auf die Daten der anderen Mandanten hat. Das vHGS ist ein von allen Teilnehmern gemeinsam genutztes System, in dem alle Kundendaten gemeinsam verwaltet werden. Es ist durch die Verknüpfung der Daten mit der mandantenbezogenen ORG-ID mandantenfähig. Im Rahmen des Service durch Dritte erfolgt aber eine gemeinsame Nutzung bestimmter Daten gemäß den Regelungen des vHGS-Vertrages.
NM	Abkürzung für Nutzermedium
Nutzer	Jeder, der ein Nutzermedium nutzt, gleichgültig ob in personalisierter oder anonymer Form
Nutzermedium	Trägermedium für die VDV-Kernapplikation. Das Nutzermedium enthält die ÖPV-Applikation. Für das eTicket RheinMain werden als Nutzermedien kontaktlose Chipkarten (nach ISO 14443) eingesetzt.
ÖPV-Applikation	Den Spezifikationen der VDV-KA entsprechende Applikation für das Nutzermedium.
Online vHGS	Aufgabenbereich im vHGS. Ein KVP mit Aufgabenbereich Online vHGS nutzt das vHGS für alle Vertriebs- und Serviceprozesse im eTicket RheinMain sowohl für eigene Kunden, als auch (im Service durch Dritte) für die Kunden anderer KVP.
Offline vHGS	Aufgabenbereich im vHGS. Im Aufgabenbereich Offline vHGS erfolgen Verkäufe von Fahrtberechtigungen im eTicket RheinMain offline zum vHGS. Service durch Dritte ist in diesem Fall nicht möglich.
ORG	Abkürzung für Organisation (hier im Sinne eines Teilnehmers am vHGS).
PH	Pflichtenheft zum vHGS
Produkt	Ein Produkt (Verkaufsprodukt) stellt ein standardisiertes Leistungsangebot dar und definiert sich durch folgende Eigenschaften: - den Leistungsanspruch, - die Produktart, - die beförderungsrechtlichen Bedingungen (z. B. Anspruchsberechtigungen wie Schülerausweis) - sowie den Produktpreis (Tarif) für den konkreten Leistungsanspruch.

Produktverantwortlicher	Der PV erwirbt vom AH das Recht zur Teilnahme am EFM-System und lässt seine Produkte dort registrieren. Er erhält vom AH die notwendigen Identifikatoren und Informationen zur Nutzung der AH-Schlüssel. Der PV bestellt im Rahmen des Sicherheitsmanagements die für die Generierung von Berechtigungen erforderlichen Schlüssel und autorisiert KVP, diese Schlüssel in seinen SAM zu nutzen. Ebenso bestellt er die zur Übertragung von Nachrichten über das ION erforderlichen Schlüssel und Zertifikate. Der Produktverantwortliche (PV) definiert die als Berechtigung auszugebenden/zu verkaufenden EFM-Produkte (siehe auch unter: Tarifverantwortlicher) und stellt diese den KVP in Form von Produktdefinitionen (Produktmodulen) und Templates zum Vertrieb bereit.
PV	Siehe Produktverantwortlicher
PVS	Produktverantwortlichensystem
pVks	Personalbediente Verkaufs- und Servicestelle im RMV. Vertriebsstelle mit direktem Kundenkontakt vor Ort.
REST Webservice	Auch RESTful Web Service. Webservice auf JAVA-Basis zur Implementierung verteilter, web-basierter Systeme.
Rollenmodell	Darstellung der Funktionsebenen (Rollen) des (((eTicket-Deutschland und möglicher Abbildungen dieser Rollen auf die beteiligten Unternehmen/Personen (Instanzen). Für die Umsetzung des (((eTicket-Systems sind die folgenden dezentral (auf der Ebene einzelner Verkehrsverbünde) organisierten Rollen erforderlich: • Produktverantwortlicher (PV) • Dienstleister (DL) • Kundenvertragspartner (KVP) • Nutzer/Kunde (N/K) Darüber hinaus existieren die folgenden zentralen Rollen: • Applikationsherausgeber (AH) • Kontrollservice (KOSE) Für die detaillierte Beschreibung der einzelnen Rollen wird auf das Dokument KA BOM-SPEC (siehe Kapitel 3, Ziffer 2 des (((eTicket-Regelwerks) der VDV-KA KG verwiesen.
SAM	Abkürzung für Secure Application Module (Sicherheitsmodul)
Sperrliste	Liste(n), die die gesperrten Objekte (Nutzermedien, Organisationen, SAM und Schlüssel) enthält (enthalten).
Sperrnachweis	Ergibt die Prüfung von Daten eines Nutzermediums gegen die im Referenzterminal vorhandene Sperrliste einen Treffer, wird das entsprechende Objekt gesperrt. Es wird ein Sperrnachweis erstellt und an die für das gesperrte Objekt verantwortliche(n) Instanz(en) und den KOSE verschickt.

Sperrmanagement	Management zur Sperrung und Entsperrung von Berechtigungen, Nutzermediumapplikationen, Schlüsseln, SAMs und Organisationen gemäß KA
Standard	Siehe VDV-Kernapplikation
Service durch Dritte	Gemeinsame KVP-übergreifende Kundenbetreuung im eTicket RheinMain
Tarifverantwortlicher	Jeder PV, der aus den Tarifen für Beförderungsleistungen eines räumlichen Gebietes, in denen unterschiedliche DL Beförderungsleistungen erbringen, Produkte entwickelt, die die vertraglichen Modalitäten zwischen ihm, dem KVP, dem DL und dem Kunden beim Verkauf von Berechtigungen und bei der Inanspruchnahme und Abrechnung von Dienstleistungen regeln (zeitliche und räumliche Gültigkeit, Personenkreis, Vergütung, Provisionen, Produktnutzungs- und ggf. -vertriebsregeln).
Teilnehmer	Alle Unternehmen, die den vHGS-Vertrag unterzeichnet haben.
Terminal	Gesamtheit der Gerätetechnik, die den Datenaustausch mit einem NM ermöglicht.
TicketShop	Aufgabenbereich im vHGS. Unternehmensübergreifender Webshop des RMV.
Transaktionsnachweis	Nachweis aus dem Aktionsmanagement, siehe auch Aktionsliste.
TX…	Transaktionsdatensatz gemäß KA. Eine detaillierte Beschreibung der TX findet sich in dem Dokument: KA SST-SPEC V1.107, Schnittstellenspezifikationen der Referenzsysteme, Kapitel 5.
TXSLNM	Sperrliste für Nutzermedien im (((eTicket Deutschland
TXSLK	Sperrliste für Schlüssel im (((eTicket Deutschland
TXSLOS	Sperrliste für Organisationen und SAMs im (((eTicket Deutschland
üfB	Übergeordnete fachliche Betriebsführung. Supporteinrichtung im Rahmen des vHGS, die für die Optimierung oder Weiterentwicklung des vHGS und für nicht zeitkritische Probleme zuständig ist.
ütB	Übergeordnete technische Betriebsführung. Supporteinrichtung im Rahmen des vHGS, die für die Behebung von Fehlern und Betriebsstörungen zuständig ist.
URL	uniform resource locator; Internetadresse oder Webadresse
VDL	Vertriebsdienstleister. Vom Teilnehmer eingesetzte Dienstleister, die die Datenverarbeitung selbständig als Verantwortlicher im datenschutzrechtlichen Sinne wahrnehmen und insoweit allein die Verantwortung für die Verarbeitung der Daten und die daraus erwachsenden datenschutzrechtlichen Pflichten, wie z. B. die Wahrnehmung der Rechte gegenüber Betroffenen, tragen.

VDV-Kernapplikation	VDV Kernapplikation; nationaler Standard für elektronisches Fahrgeldmanagement (EFM) in Deutschland. Die VDV-Kernapplikation ermöglicht es, ein NM als Speichermedium für EFS, als Legitimationsmedium für eine (((eBezahlberechtigung und / oder als Erfassungsmedium für die Automatisierte Fahrpreisermittlung einzusetzen.
VDV-KA	Siehe VDV-Kernapplikation
VDV-KA KG	VDV-Kernapplikations GmbH & Co. KG, Köln
VDV-KA Spezifikation	Siehe VDV-Kernapplikation
Vertragspartner	Vertragspartner im vHGS sind der jeweilige Teilnehmer und der RMV
vHGS	verbundweites Hintergrundsystem zur Umsetzung des Elektronischen Fahrgeldmanagements (EFM) einschließlich des Service durch Dritte im Verbundgebiet des RMV
Vertrieb JobTicket ohne Service durch Dritte	Aufgabenbereich im vHGS. Im Aufgabenbereich Vertrieb JobTicket ohne Service durch Dritte nutzen Teilnehmer das vHGS alleine für die Verwaltung und Ausgabe von JobTickets an Mitarbeiter des JobTicketunternehmens. In diesem Fall findet kein Service durch Dritte statt.
Web-Frontend	Browserbasierte Eingabemaske zur Eingabe von Daten in das vHGS bzw. zum Auslesen von Daten aus dem vHGS.
XML	extensible markup language. XML ist ein Standard zur Strukturierung von Dokumenten im Internet und wird für den plattform- und implementationsunabhängigen Austausch von Daten genutzt.
XML-Schema	Empfehlung zur Definition von Strukturen für XML-Dokumente.
XSD	XML-Schema Definition (siehe XML).
Zentrale Vermittlungsstelle	Von der VDV-KA KG als Applikationsherausgeberin des (((eTicket Deutschland betriebene Vermittlungsstelle im ION. Zentrale Systeme, die deutschlandweit nur einmal existieren, sind direkt an der Zentralen Vermittlungsstelle angeschlossen (KOSES, AHS). Regionale (((eTicket-Systeme werden im ION mittels Regionaler Vermittlungsstellen an die Zentrale Vermittlungsstelle angeschlossen.
Zertifikat	Digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten (hier: relevanten Systemkomponenten des elektronischen Fahrgeldmanagements) bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.

Anmerkungen:

In diesem Glossar nicht aufgeführte Abkürzungen und Fachbegriffe, aus dem Vertrag über die Teilnahme am (((eTicket Deutschland sind im dortigen Glossar [siehe: Kapitel 1 zum (((eTicket-Regelwerk] erläutert.

Erläuterungen zu Begriffen, die nicht vHGS-spezifisch sind, sind überwiegend aus der Dokumentation zur VDV-Kernapplikation (insbesondere KA-Glossar V1.107) übernommen.

RHEIN-MAIN-VERKEHRSVERBUND

Auszug aus (((eTicket-TNV RMV

Auszug aus (((eTicket-Teilnahmevertrag
zwischen VDV-ETS KG
und RMV

Anlage 9 zum vHGS-Vertrag

Thema:	Auszug aus (((eTicket Teilnahmevertrag des RMV
Dateiname:	Anlage 9_Auszug aus (((eTicket-TNV RMV
Erstellt am:	08.12.2011
Zuletzt geändert am:	08.12.2011
Version:	1.0
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Auszug der RMV-spezifischen Inhalte aus dem „Vertrag über die Teilnahme am (((eTicket-Deutschland“ zwischen VDV-KA KG und RMV vom 01.11.2011 (als Anlage zum vHGS-Vertrag V1.0).

Auszug aus:

(((eTicket-Teilnahmevertrag

Vertrag über die Teilnahme am (((eTicket-Deutschland

zwischen

VDV eTicket Service GmbH & Co. KG
Hohenzollernring 103
50672 Köln

- nachstehend „VDV-ETS KG“ genannt -

und

Rhein-Main-Verkehrsverbund GmbH
Alte Bleiche 5
65719 Hofheim a.Ts.

- nachstehend „Teilnehmer“ genannt -

§ 1
Vertragsgegenstand

1. Der Teilnehmer wird in den nachfolgend gekennzeichnete(n) Rolle(n) am (((eTicket-Deutschland teilnehmen (Mehrfachnennungen sind möglich):

   ☒ Produktverantwortlicher

   ☐ Dienstleister

   ☐ Kundenvertragspartner

§ 4
Abweichungen von den Regelungen des (((eTicket-Teilnahmevertrags und des (((eTicket-Regelwerks während des Migrationszeitraums

Zur Erreichung der Interoperabilität verfolgen der Teilnehmer und die VDV-ETS KG das Ziel, dass in jeder Ausbauvariante eine (((eBezahlberechtigung an jeden Kunden ausgegeben wird, die jedem Kunden den Erwerb von Fahrscheinen bei Teilnehmern mit den Ausbauvarianten „(((eBezahlen“ und „(((eFahrschein mit (((eKontrolle“ und die Inanspruchnahme von Beförderungsleistungen bei Teilnehmern mit der Ausbauvariante „Automatisierte Fahrpreisermittlung“ ermöglicht.

Die Parteien vereinbaren nachfolgende Abweichungen von den Regelungen des (((eTicket-Teilnahmevertrags und den (((eTicket-Teilnahmebedingungen (Kapitel 2 des (((eTicket-Regelwerks):

1. Der Teilnehmer wird zunächst ab 01.01.2012 Jahreskarten und Jahresabonnements, jeweils im Erwachsenentarif, als elektronische Fahrscheine anbieten.
   Ab dem 01.01.2013 werden zusätzlich Wochen- und Monatskarten, jeweils sowohl im Erwachsenen-, als auch im Ausbildungstarif als elektronische Fahrscheine angeboten.
   Vom 01.01.2014 an werden Einzelfahrscheine sowie Tages- und Gruppenkarten als elektronische Fahrscheine angeboten. Es werden zu diesem Zeitpunkt jedoch noch keine Nutzermedien an Gelegenheitskunden für Einzelfahrten ausgegeben.
   Ab 2014 wird der Teilnehmer sämtliche (((eBezahlberechtigungen akzeptieren und selbst eine POB ausgeben.

   Der Teilnehmer wird zunächst nicht den KOSE und die zentrale Vermittlungsstelle nutzen. Ein Anschluss an den KOSE und die zentrale Vermittlungsstelle ist für 2012 geplant.

2. § 3 Abs. 3 h) und l) und § 3 Nr. 4 k) der (((eTicket-Teilnahmebedingungen findet erst Anwendung, wenn der Teilnehmer dem Clearingvertrag beigetreten ist.

3. § 3 Abs. 4 c), d) und e) der (((eTicket-Teilnahmebedingungen finden bis auf weiteres keine Anwendung.

4. **Migrationsregelung Ausbauvariante 2 a (ab 2012)**
   (nur Abonnements als (((eFahrschein):

   Abweichend von § 1 Abs. 2 Satz 1 TNV ist der Teilnehmer bis zu dem dort genannten Datum zur Umsetzung der gemäß § 1 Abs. 3 TNV gewählten Ausbauvariante „(((eFahrschein mit (((eKontrolle“ nur im Hinblick auf elektronische Abonnement-Zeitfahrausweise verpflichtet.
   Der Teilnehmer beabsichtigt ab dem 01.01.2012 die Ausgabe von Abonnements als EFS.
   Eine vollständige Umsetzung der gemäß § 1 Abs. 3 TNV gewählten Ausbauvariante „(((eFahrschein mit (((eKontrolle“ wird voraussichtlich bis 2014 erfolgen. Der Zeitraum zwischen dem in Satz 2 und dem in Satz 3 dieses Absatzes genannten Datum wird nachfolgend als **„Migrationszeitraum“** bezeichnet.

Während des Migrationszeitraums gelten abweichend von Kapitel 3 des (((eTicket-Regelwerks die in der Anlage 2 zu diesem (((eTicket-Teilnahmevertrag aufgeführten Elementarprozesse und Anwendungsfälle für (((eTicket-Systemkomponenten in ihrer jeweils gültigen Fassung.

Der Teilnehmer ist während des Migrationszeitraums abweichend von § 3 Abs. 3 a) der (((eTicket-Teilnahmebedingungen nicht verpflichtet, an seine Kunden eine (((eBezahlberechtigung auszugeben und abweichend von § 3 Abs. 3 c) der (((eTicket-Teilnahmebedingungen nicht verpflichtet, (((eBezahlberechtigungen zu akzeptieren. Jedoch müssen das dem Kunden ausgegebene Nutzermedium sowie der Teilnehmer, der das Nutzermedium und die Applikation ausgegeben hat, das Aufbringen von Elektronischen Fahrscheinen sowie einer (((eBezahlberechtigung durch einen anderen Kundenvertragspartner als dem Teilnehmer zulassen..

§ 3 Nr. 3 e), g), h) und l), § 3 Nr. 4 f), g) und i) sowie § 3 Nr.5 c) des (((eTicket-Regelwerks, Kapitel 2 finden in dieser Ausbauvariante keine Anwendung.

5. **Migrationsregelung Ausbauvariante 2 b (ab 2014)**
(regional begrenzte Akzeptanz von (((eBezahlberechtigungen)

Abweichend von § 1 Abs. 2 Satz 1 TNV ist der Teilnehmer bis zu dem dort genannten Datum zur Umsetzung der gemäß § 1 Abs. 3 TNV gewählten Ausbauvariante „(((eFahrschein mit (((eKontrolle“ nur im Hinblick auf die Akzeptanz von (((eBezahlberechtigungen aus dem Einflussbereich seines PV´s verpflichtet. Es steht dem Teilnehmer frei, (((eBezahlberechtigungen aus weiteren Regionen zu akzeptieren.
Der Teilnehmer beabsichtigt ab 2014 die Ausgabe von EFS (über Abonnements hinaus).
Eine vollständige Umsetzung der gemäß § 1 Abs. 3 TNV gewählten Ausbauvariante „(((eFahrschein mit (((eKontrolle“ wird voraussichtlich bis 2016 erfolgen. Vollständige Umsetzung bedeutet in diesem Fall die Ausgabe einer überregional einsetzbaren (((eBezahlberechtigung und die Akzeptanz aller (((eBezahlberechtigungen zum Kauf möglichst aller Tarifprodukte. Der Zeitraum zwischen dem in Satz 3 und dem in Satz 4 dieses Absatzes genannten Datum wird nachfolgend als **„Migrationszeitraum“** bezeichnet. Dieser Migrationszeitraum löst in seiner Geltung den unter § 4 Abs. 3, S.4 genannten Migrationszeitraum ab.

Während des Migrationszeitraums gelten abweichend von Kapitel 3 des (((eTicket-Regelwerks die in der Anlage 2 zu diesem (((eTicket-Teilnahmevertrag aufgeführten Elementarprozesse und Anwendungsfälle für (((eTicket-Systemkomponenten in ihrer jeweils gültigen Fassung.

Der Teilnehmer ist während des Migrationszeitraums abweichend von § 3 Abs. 3 a) der (((eTicket-Teilnahmebedingungen nur verpflichtet, jedem Kunden eine (((eBezahlberechtigung auszugeben, die dieser innerhalb des Einflussbereichs seines PV´s zum Erwerb von elektronischen Fahrscheinen und Papierfahrscheinen einsetzen kann.

§ 3 Nr.5 c) des (((eTicket-Regelwerks, Kapitel 2 findet in dieser Ausbauvariante keine Anwendung

RHEIN-MAIN-VERKEHRSVERBUND

Technische und organisatorische Maßnahmen
rms GmbH

Anlage 10 zum vHGS-Vertrag

RHEIN-MAIN-VERKEHRSVERBUND

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.2	rms	06.08.2018	Version als Anlage zum vHGS-Vertrag V1.1

Dokumentation der technischen und organisatorischen Maßnahmen

Nach Art. 32 Abs. 1 DSGVO

der

Rhein-Main-Verkehrsverbund Servicegesellschaft mbH
Am Hauptbahnhof 6
60329 Frankfurt am Main

(„rms GmbH")

Stand: 06. August 2018

Version: 1.2

Inhaltsverzeichnis

Technisch-organisatorische Maßnahmen

Stand: 06. Juli 2018

Version: 1.1

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung hat der Verantwortliche folgende technische und organisatorische Maßnahmen getroffen:

1. Pseudonymisierung

Eine Pseudonymisierung ist gegeben, wenn die Merkmale der Datensätze, die ihn hinsichtlich einer Person bestimmt oder bestimmbar werden lassen, nach festgelegten Regeln durch Pseudonyme ersetzt werden. Derartige Maßnahmen werden derzeit nicht eingesetzt.

„Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Abs. 5 DSGVO, siehe auch Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

2. Verschlüsselung

Zum Schutz der Integrität und Vertraulichkeit der verarbeiteten Daten, sind diese mit kryptografischen Verfahren zu schützen, die sich am Stand der Technik orientieren.

Verschlüsselung ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“, so dass der Klartext aus dem Geheimtext nur utner Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können (siehe auch Art. 32 Abs. 1 lit. a DSGVO)

Die rms GmbH setzt in folgender Weise Verschlüsselung zum Schutz personenbezogener Daten ein.

- Werden Daten auf einem Datenträger außerhalb der Geschäftsfläche transportiert, werden diese Daten verschlüsselt, um den Zugriff auf die Daten bei Verlust eines Datenträgers durch Unbefugte zu schützen.
- Werden Daten elektronisch übermittelt, werden diese vor der Übermittlung verschlüsselt. Eine Ausnahme hiervon ist die Übertragung von Daten über bereits verschlüsselte Transportwege (z.B. VPN oder SSL-Verbindung).
- Der externe Zugriff auf Daten erfolgt ausschließlich über verschlüsselte Verbindungen (z.B. VPN- oder SSL-Verbindungen).

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Vertraulichkeit ist gewährleistet, wenn die von einem System verarbeiteten Daten nicht unbefugt zur Kenntnis genommen, nicht aufgezeichnet und auch sonst nicht verwendet werden können.

Laut dem Bundesamt für Sicherheit und Informationstechnik ist der Begriff „Vertraulichkeit“ wie folgt definiert:

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

In diesem Abschnitt wird erläutert, wie die rms GmbH Vertraulichkeit im Umgang mit den relevanten Daten sicherstellt.

3.1. Zutrittskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle), (Anlage zu § 9 Satz 1 BDSG alt).

Die rms GmbH ergreift folgende Maßnahmen, um den Zutritt Unbefugter zu Gebäuden und Räumlichkeiten zu verhindern.

3.1.1. Zugang in das Gebäude - Haupteingang

- Der Haupteingang ist mit einem Schließsystem ausgestattet. Der Zutritt zum Gebäude über den Haupteingang ist nur mit einem Schlüssel möglich. Jeder Mietpartei werden entsprechende Schlüssel zum Zutritt des Gebäudes bereitgestellt.
- Der Haupteingang verfügt über ein videobasiertes Türöffnungssystem.
- Die Eingangstüren bestehen aus einer soliden Metallkonstruktion und massivem Glas

3.1.2. Andere Zugänge in das Gebäude – Parkplatz und Nebeneingang

- Das Gebäude verfügt über einen Parkplatz, der über eine Einfahrt zugänglich ist. Die Einfahrt ist durch ein elektronisches Rolltor ausgestattet. Das Rolltor ist verschlossen und kann mit einer Fernbedienung geöffnet werden. Jeder Mitpartei, die über einen angemieteten Parkplatz verfügt, wird eine entsprechende Fernbedienung ausgehändigt.
- In diesem Rolltor befindet sich eine Tür, die mit dem Generalschlüssel, der auch die Eingangstüren des Haupt- und Nebeneinganges schließt, zugänglich gemacht wird.
- Das Gebäude verfügt über einen Nebeneingang mit Zugang zum Nebentreppenhaus. Der Nebeneingang ist mit einem Schließsystem ausgestattet. Der Zutritt zum Nebeneingang ist nur mit einem Schlüssel möglich. Jeder Mietpartei werden entsprechende Schlüssel zum Zutritt des Nebeneingangs bereitgestellt.
- Der Nebeneingang verfügt über ein videobasiertes Türöffnungssystem.
- Der Zugang zum Nebentreppenhaus ist im Erdgeschoss mit einer Tür aus Metallverstrebungen geschützt. Die Tür ist mit einem Schließsystem ausgestattet. Jeder

Mietpartei werden entsprechende Schlüssel zum Zutritt des Nebentreppenhauses bereitgestellt.
- Das Gebäude verfügt im Nebentreppenhaus über einen Fahrstuhl. Der Fahrstuhl verfügt über ein Schließsystem und kann zwischen 21:00 Uhr abends und 06:00 Uhr morgens nur mit einem entsprechenden Schlüssel bedient werden. Jeder Mietpartei werden entsprechende Schlüssel zur Bedienung des Fahrstuhls bereitgestellt.

3.1.3. Zugang zur Geschäftsfläche

- Die Geschäftsfläche verfügt über mehrere Haupt- und Nebeneingänge.
- Die Eingänge sind mit einem Schließsystem ausgestattet. Der Zutritt zur Geschäftsfläche ist nur mit einem Schlüssel möglich. Festangestellte Mitarbeiter der rms GmbH mit festem Arbeitsvertrag, Studenten und Zeitarbeitskräfte und Dienstleister der rms GmbH (z.B. Putzpersonal) verfügen über einen entsprechenden Schlüssel.
- Die Haupteingänge zur Geschäftsfläche verfügen über ein videobasiertes Türöffnungssystem.
- Die Eingangstüren zur Geschäftsfläche bestehen aus Metall, Kunststoff und massivem Glas.

3.1.4. Zugang zu den Büroräumen

- Die Eingangstüren zu den Büroräumen innerhalb der Geschäftsfläche sind mit einem Schließsystem ausgestattet. Jeder Mitarbeiter erhält einen Schlüssel zu seinem Büro.
- Die Bürotüren werden abgeschlossen, wenn das Büro verlassen wird und sich kein weiterer Mitarbeiter im Büro befindet.
- Die Eingangstüren zu den Büroräumen bestehen aus massivem Holz.
- Das GF-Sekretariat verfügt über Generalschlüssel für alle Eingangstüren- und Büros.

3.1.5. Zugang zum Serverraum

- Die Tür zum Serverraum ist mit einem Schließsystem ausgestattet. Ausschließlich Mitarbeiter der IT-Abteilung verfügen über einen entsprechenden Schlüssel.
- Die Tür zum Serverraum besteht aus massivem Holz.

3.1.6. Besuche und Dienstleister

- Besucher werden an der Eingangstür durch den Empfang / die EmpfangsmitarbeiterInnen empfangen.
- Externe Dienstleister können sich nur in Begleitung eines Mitarbeiters der rms GmbH auf der Geschäftsfläche bewegen, um ihrer vereinbarten Tätigkeit nachzukommen. Eine Ausnahme ist das Reinigungs- und Wachpersonal, das sich ohne Begleitung eines Mitarbeiters der rms GmbH auf der Geschäftsfläche bewegen darf.
- Werden Wartungs- oder Instandsetzungsarbeiten in der Nacht oder am Wochenende erforderlich, werden diese Arbeiten durch Wachpersonal überwacht.

3.1.7. Organisatorische Regelungen über Zugangsberechtigungen zum Geschäftsbereich

- Festangestellte Mitarbeiter mit festem Arbeitsvertrag erhalten einen Schlüssel für den Zugang in das Gebäude und die Geschäftsfläche.
- Jeder Mitarbeiter erhält einen Schlüssel zu seinem Büro.
- Dienstleister (z.B. Wach- und Putzpersonal) erhalten zur Ausübung ihrer vertraglich vereinbarten Leistung bei Bedarf einen Schlüssel zu den erforderlichen Flächen und Räumen.
- Das Sekretariat führt eine Dokumentation der Schlüssel, die an Mitarbeiter und Dienstleister ausgegeben werden.
- Bei Verlust eines Schlüssels wird geprüft, ob eine Zuordnung des Schlüssels zur Bürofläche möglich ist. Ist dies der Fall, wird ein neues Schließsystem eingebaut und neue Schlüssel ausgegeben.

3.2. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (§ 64 Abs. 3 Nr. 1 BDSG (Neu))

Die rms GmbH ergreift folgende Maßnahmen, um zu verhindern, dass Unbefugte Zugang zu IT-Systemen erhalten.

3.2.1. Authentifikation von Benutzern

- Der Zugang zu Computersystemen erfordert eine zentrale Authentifizierung im Netzwerk (Active Directory Domain Services).
- Zur erfolgreichen Authentifizierung ist ein Benutzername und Kennwort erforderlich.
- Passwortkonventionen:
  - Mindestlänge 8 Zeichen
  - Keine Trivialkennworte
  - Maximal 90 Tage Gültigkeitsdauer
  - Hohe Zahl der Generationen
  - Sperrung bei wiederholter Fehleingabe

3.2.2. Schutz vor unbefugtem Zugriff

- Die Benutzerkontenverwaltung (Erstellen und Verwalten von Benutzerkonten) erfolgt zentral durch Mitarbeiter der IT-Abteilung. Der Zugriff auf die Verwaltungskonsolen, der administrative Zugang zu den Serversystemen und der Zugang zu den Serverräumen sind ausschließlich Mitarbeitern der IT-Abteilung vorbehalten.
- Fehlgeschlagene Anmeldeversuche werden protokolliert und ausgewertet. Bei Bedarf werden notwendige Maßnahmen zum Schutz der IT-Umgebung eingeleitet.

3.3. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung

Die rms GmbH ergreift folgende Maßnahmen, um den unbefugten Zugriff auf personenbezogene Daten zu verhindern.

3.3.1. Berechtigungskonzept

- Der IT-Infrastruktur liegt ein Berechtigungskonzept zugrunde, über das der Zugriff auf Daten im Netzwerk reglementiert wird. Auf diese Weise wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Der Zugriff auf Daten wird über Berechtigungen gesteuert, die einem Benutzerkonto zugewiesen werden. Hierbei kann es sich z.B. um NTFS-, Freigabe oder Datenbankberechtigungen handeln.

3.3.2. Organisatorische Regelungen

- Werden Zugangsberechtigungen für einen Mitarbeiter benötigt, werden diese vom jeweiligen Vorgesetzten eines Mitarbeiters schriftlich bei der IT-Abteilung angefragt. Die IT-Abteilung prüft die Anfrage und weist die angeforderten Zugangsberechtigungen dem Benutzerkonto des Mitarbeiters zu.
- Es kann jederzeit zweifelsfrei festgestellt werden, welchen Mitarbeitern Zugriffsberechtigungen auf einen bestimmten Datensatz zur Verfügen gestellt wurden.

3.3.3. Dedizierte Speicherorte

- Um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, findet eine Trennung der Daten durch das Einrichten dedizierter Ablageorte (z.B. dedizierte Freigaben, Ordner oder Datenbanken) und einer gezielten Vergabe von Berechtigungen statt (Berechtigungskonzept).

3.4. Weitergabekontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogenen Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle) (§ 64 Abs. 3 Nr. 6 BDSG (neu))

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle) (§ 64 Abs. 3 Nr. 8 BDSG (neu))

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle) (§ 64 Abs. 3 Nr. 2 BDSG (neu))

Die rms GmbH ergreift folgende Maßnahmen, um den unbefugten Zugriff auf personenbezogene Daten bei Übertragung, Transport oder Speicherung auf Datenträger zu verhindern und zu gewährleisten, dass überprüfbar ist, an wen eine Übermittlung personenbezogener Daten vorgesehen ist.

3.4.1. Datenträger

- Datenträger werden geschützt vor dem Zugriff Unbefugter aufbewahrt. Je nachdem, welche Daten auf den Datenträgern gespeichert sind, werden diese in einem abschließbaren Schrank, einem abschließbaren Rollcontainer oder einem Sicherheitsschrank verwahrt.
- Im Unternehmen werden Datenschutz-Tonnen vorgehalten. Die Schlüssel hierzu werden in der internen Schüsselverwaltung aufbewahrt.
- Der Serverraum ist von der zentralen Schlüsselverwaltung ausgenommen.
- Werden Daten auf einem Datenträger außerhalb der Geschäftsfläche transportiert, werden diese Daten verschlüsselt, um den Zugriff auf die Daten bei Verlust eines Datenträgers durch Unbefugte zu schützen.
- Werden Datenträger außerhalb der Geschäftsfläche aufbewahrt (z.B. Sicherungskopien auf LTO-Medien), werden diese in einem Sicherheitsschrank verwahrt.
- Werden Datenträger nicht mehr benötigt und entsorgt, wird ein externes Unternehmen mit der professionellen Vernichtung der Datenträger beauftragt. Ein Mitarbeiter der rms GmbH überwacht die Vernichtung der Datenträger. Die Vernichtung der Datenträger wird schriftlich in einem Protokoll festgehalten.

3.4.2. Datenversand

- Werden Daten elektronisch übermittelt, werden diese vor der Übermittlung verschlüsselt. Eine Ausnahme hiervon ist die Übertragung von Daten über bereits verschlüsselte Transportwege (z.B. VPN oder SSL-Verbindung).

3.4.3. Externer Zugriff

- Der externe Zugriff auf Daten erfolgt ausschließlich über verschlüsselte Verbindungen (z.B. VPN- oder SSL-Verbindungen).

- Für den externen Zugriff über VPN sind ein Zertifikat und ein Kennwort erforderlich, das ausschließlich von Mitarbeitern der IT-Abteilung bereitgestellt werden kann. Nachdem einem erfolgreichen Verbindungsaufbau ist die zentrale Authentifizierung im Netzwerk erforderlich

3.5. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (§ 64 Abs. 3 Nr. 7 BDSG (neu))

Die rms GmbH ergreift folgende Maßnahmen, um die Überprüfbarkeit von Eingaben, Änderungen und Löschungen personenbezogener Daten in IT-Systemen zu gewährleisten.

- Mittels Benutzeridentifikation und Protokollierung ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

3.6. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (§ 64 Abs. 3 Nr. 14 BDSG (neu))

Die rms GmbH ergreift die folgenden allgemeinen Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

- Damit zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, findet eine Trennung der Daten durch das Einrichten dedizierter Ablageorte (z.B. dedizierte Freigaben, Ordner oder Datenbanken) und einer gezielten Vergabe von Berechtigungen statt (Berechtigungskonzept).

4. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten […] Es drückt aus, dass die Daten vollständig und unverändert sind (BSI).

Viele der bereits in Kapitel 3 „Vertraulichkeit“ beschriebenen Maßnahmen dienen ebenfalls dazu, die Integrität personenbezogener Daten sicherzustellen.

4.1. Zugang zum Serverraum

- Die Tür zum Serverraum ist mit einem Schließsystem ausgestattet. Ausschließlich Mitarbeiter der IT-Abteilung verfügen über einen entsprechenden Schlüssel.
- Die Tür zum Serverraum besteht aus massivem Holz.

4.2. Authentifikation von Benutzern

- Der Zugang zu Computersystemen erfordert eine zentrale Authentifizierung im Netzwerk (Active Directory Domain Services).
- Zur erfolgreichen Authentifizierung ist ein Benutzername und Kennwort erforderlich.
- Passwortkonventionen
  - Mindestlänge 8 Zeichen
  - Keine Trivialkennworte
  - Maximal 90 Tage Gültigkeitsdauer
  - Hohe Zahl der Generationen
  - Sperrung bei wiederholter Fehleingabe

4.3. Schutz vor unbefugtem Zugriff

- Die Benutzerkontenverwaltung (Erstellen und Verwalten von Benutzerkonten) erfolgt zentral durch Mitarbeiter der IT-Abteilung. Der Zugriff auf die Verwaltungskonsolen, der administrative Zugang zu den Serversystemen und der Zugang zu den Serverräumen sind ausschließlich Mitarbeitern der IT-Abteilung vorbehalten.
- Fehlgeschlagene Anmeldeversuche werden protokolliert und ausgewertet. Bei Bedarf werden notwendige Maßnahmen zum Schutz der IT-Umgebung eingeleitet.

4.4. Berechtigungskonzept

- Der IT-Infrastruktur liegt ein Berechtigungskonzept zugrunde, über das der Zugriff auf Daten im Netzwerk reglementiert wird. Auf diese Weise wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Der Zugriff auf Daten wird über Berechtigungen gesteuert, die einem Benutzerkonto zugewiesen werden. Hierbei kann es sich z.B. um NTFS-, Freigabe oder Datenbankberechtigungen handeln.

4.5. Organisatorische Regelungen

- Werden Zugangsberechtigungen für einen Mitarbeiter benötigt, werden diese vom jeweiligen Vorgesetzten eines Mitarbeiters schriftlich bei der IT-Abteilung angefragt. Die IT-Abteilung prüft die Anfrage und weist die angeforderten Zugangsberechtigungen dem Benutzerkonto des Mitarbeiters zu.
- Es kann jederzeit zweifelsfrei festgestellt werden, welchen Mitarbeitern Zugriffsberechtigungen auf einen bestimmten Datensatz zur Verfügen gestellt wurden.

4.6. Externer Zugriff

- Der externe Zugriff auf Daten erfolgt ausschließlich über verschlüsselte Verbindungen (z.B. VPN- oder SSL-Verbindungen).
- Für den externen Zugriff über VPN sind ein Zertifikat und ein Kennwort erforderlich, das ausschließlich von Mitarbeitern der IT-Abteilung bereitgestellt werden kann. Nachdem einem erfolgreichen Verbindungsaufbau ist die zentrale Authentifizierung im Netzwerk erforderlich (siehe C.1.)
- Schutz vor unberechtigten Netzwerkzugriffen
- Das Netzwerk der rms ist von außen durch redundant ausgelegte, moderne Firewall-Systeme geschützt.
- Im internen Netzwerk der rms wird der Zugriff auf wichtige IT Systeme ebenfalls durch eine redundant ausgelegte Firewall geschützt.
- Zusätzlich zu den dedizierten externen und internen Firewalls werden die auf Serversystemen integrierten Firewalls zum Schutz der Serversysteme aktiviert und konfiguriert.
- Die Firewall-Regeln werden in regelmäßigen Abständen überprüft. Eine Kontrolle der Firewall-Logs wird in regelmäßigen Abständen durchgeführt, um unautorisierte Zugriffsversuche zu erkennen.

4.7. Schutz vor Schadsoftware

- Die rms setzt leistungsstarke Software zum Schutz vor Schadsoftware ein.
- Serversysteme und Clients sind mit einem zentral verwalteten Schutzprogramm ausgestattet, das unter anderem nachfolgende Merkmale aufweist: Machine Learning, Verhaltensanalyse, Datei-Reputation, Schutz gegen Varianten, Web-Schutz und Exploit-Schutz.
- Der Schutz vor schadhaften E-Mails ist mehrstufig aufgebaut. In der ersten Stufe werden eingehende E-Mails von einem dedizierten System auf Schadsoftware, SPAM- und Phishing-E-Mails überprüft. Bekannte SPAM-Versender werden über Reputationsdatenbanken auf IP-Ebene geblockt, bevor E-Mails übermittelt werden können. Wird keine Bedrohung gefunden, werden die E-Mails an die internen E-Mailserver weitergeleitet. Auf den E-Mailservern ist spezielle Software installiert, die eingehende E-Mails erneut auf Schadsoftware überprüft. Öffnet ein Benutzer eine E-Mail auf seinem Client, wird der Inhalt der E-Mail und die Anhänge auf dem Client durch ein weiteres Produkt auf schadhafter Software überprüft.

4.8. Sicherheitsupdates / Softwareupdates / Firmwareupdates

- Wesentlicher Bestandteil zum Schutz vor Schadsoftware ist das Einspielen von sicherheitsrelevanten Updates. Diese werden umgehend nach Erscheinen auf den Server- und Clientsystemen installiert.
- Software- und Firmwareupdates die nicht sicherheitsrelevant sind, werden ebenfalls in regelmäßigen Abständen eingespielt.

5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

5.1. Verfügbarkeitskontrolle

Zur Gewährleistung der Verfügbarkeit sind Maßnahmen zu treffen, die sicherstellen sollen, dass das System stets wie vorgesehen genutzt werden kann, d.h. Maßnahmen zum Schutz vor (zufälligem) Verlust oder Zerstörung der Daten.

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (§ 64 Abs. 3 Nr. 13 BDSG (neu))

Die rms GmbH ergreift folgende Maßnahmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen.

5.1.1. Brandschutz

- Die Geschäftsfläche ist mit Brandmeldern ausgestattet, die an eine Brandmeldezentrale angeschlossen sind.
- Beim Auslösen eines Rauchmelders wird automatisch ein Notruf an die Feuerwehr abgesetzt.
- Die Geschäftsfläche ist in mehrere Brandabschnitte unterteilt.

5.1.2. Serverräume

- Die Serverräume sind mit redundanten, unterbrechungsfreien Stromversorgungen ausgestattet, die kurze Stromausfälle abfangen und die Hardware vor Spannungsschwankungen schützen.
- Die Serverräume sind mit redundanten Klimageräten ausgestattet. Es ist eine Temperaturüberwachung der Serverräume eingerichtet, die beim Überschreiten einer vorgegebenen Temperatur einen Alarm auslöst und eine SMS an die Mitarbeiter der IT-Abteilung versendet.

5.1.3. Datensicherung

- Sicherungskopien der Daten werden regelmäßig in einen gesonderten Brandabschnitt repliziert.
- Zusätzlich werden Sicherungskopien auf externen Datenträgern angefertigt und außerhalb der Geschäftsfläche aufbewahrt.

5.1.4. Schutz vor unberechtigten Netzwerkzugriffen

- Das Netzwerk der rms GmbH ist von außen durch redundant ausgelegte, moderne Firewall-Systeme geschützt.
- Im internen Netzwerk der rms GmbH wird der Zugriff auf wichtige IT Systeme ebenfalls durch eine redundant ausgelegte Firewall geschützt.
- Zusätzlich zu den dedizierten externen und internen Firewalls werden die auf Serversystemen integrierten Firewalls zum Schutz der Serversysteme aktiviert und konfiguriert.

- Die Firewall-Regeln werden in regelmäßigen Abständen überprüft. Eine Kontrolle der Firewall-Logs wird in regelmäßigen Abständen durchgeführt, um unautorisierte Zugriffsversuche zu erkennen.

5.1.5. Schutz vor Schadsoftware

- Die rms GmbH setzt leistungsstarke Software zum Schutz vor Schadsoftware ein.
- Serversysteme und Clients sind mit einem zentral verwalteten Schutzprogramm ausgestattet, das unter anderem nachfolgende Merkmale aufweist: Machine Learning, Verhaltensanalyse, Datei-Reputation, Schutz gegen Varianten, Web-Schutz und Exploit-Schutz.
- Der Schutz vor schadhaften E-Mails ist mehrstufig aufgebaut. In der ersten Stufe werden eingehende E-Mails von einem dedizierten System auf Schadsoftware, SPAM- und Phishing-E-Mails überprüft. Bekannte SPAM-Versender werden über Reputationsdatenbanken auf IP-Ebene geblockt, bevor E-Mails übermittelt werden können. Wird keine Bedrohung gefunden, werden die E-Mails an die internen E-Mailserver weitergeleitet. Auf den E-Mailservern ist spezielle Software installiert, die eingehende E-Mails erneut auf Schadsoftware überprüft. Öffnet ein Benutzer eine E-Mail auf seinem Client, wird der Inhalt der E-Mail und die Anhänge auf dem Client durch ein weiteres Produkt auf schadhafter Software überprüft.

5.1.6. Sicherheitsupdates / Softwareupdates / Firmwareupdates

- Wesentlicher Bestandteil zum Schutz vor Schadsoftware ist das Einspielen von sicherheitsrelevanten Updates. Diese werden umgehend nach Erscheinen auf den Server- und Clientsystemen installiert.
- Software- und Firmwareupdates die nicht sicherheitsrelevant sind, werden ebenfalls in regelmäßigen Abständen eingespielt.

5.1.7. Backups

- Die rms GmbH führt in regelmäßigen Abständen eine Datensicherung durch, damit durch diesen redundanten Datenbestand der IT-Betrieb kurzfristig wieder aufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Im nachfolgenden wird das Datensicherungskonzept skizziert.

5.1.8. Serversysteme

- Die für das operative Geschäft eingesetzten Serversysteme sind virtualisiert. Im Rahmen der Datensicherung wird direkt nach Inbetriebnahme eines Serversystems eine Datensicherung der virtuellen Maschine erstellt. Werden Änderungen an der Konfiguration der virtuellen Maschine durchgeführt, erfolgt eine erneute Datensicherung der virtuellen Maschine.

5.1.9. Produktivdaten

- Zusätzlich zur Datensicherung der virtuellen Maschine werden die Produktivdaten innerhalb einer virtuellen Maschine in Abhängigkeit von der Art der Daten gesichert. Die Sicherung erfolgt je nach Datenmenge als Vollbackup, oder als Vollbackup mit anschließenden inkrementellen Backups.
- Je nach Art der Daten wird eines der folgenden Sicherungsintervalle angewendet:
  - Täglich eine Sicherungskopie der Daten an Werktagen.
  - Täglich eine Sicherungskopie der Daten (Mo-So., auch Feiertage).
  - Täglich zwei Sicherungskopien der Daten (Mo-So., auch Feiertage).
- Die Datensicherung der Produktivdaten wird für zwei Wochen vorgehalten. Am Ende des Monats wird eine Datensicherung mit allen Produktivdaten auf Sicherungsbändern (LTO-Medien) erstellt, die gemäß den Nutzungsbestimmungen bzw. gesetzlichen Vorschriften außerhalb des Firmengeländes aufbewahrt wird.

5.1.10. Dauer der Aufbewahrung

- Die Dauer der Aufbewahrung einer Datensicherung variiert. Grundsätzlich werden folgende Aufbewahrungsfristen eingehalten:
  - 2 Wochen für sämtliche Produktivdaten
  - 1 Jahr für die Datensicherung am Monatsende
  - 2 Jahre für bestimmte Daten wie bspw. Projektdaten
  - 2-10 Jahre nach Gesetz bzw. nach Vereinbarung

5.1.11. Schutz / Auslagerung der Sicherungsmedien

- Die Serversysteme mit den Produktivdaten der rms GmbH befinden sich im Serverraum des 4.OG für den Standort Frankfurt und im Serverraum des 4.OG für den Standort Berlin. Das Backupsystem für beide Standorte befindet sich im Serverraum des 2.OG am Standort Frankfurt und ist in einem von den Produktivsystemen abgetrennten Brandabschnitt untergebracht.
- Die Monats- und Jahressicherungsmedien werden nach Erstellen einer Sicherungskopie außerhalb der Geschäftsräume der rms GmbH sicher verwahrt. Somit ist ausgeschlossen, dass ein Brand oder eine andere Katastrophe die Sicherungskopien zerstört.

5.1.12. Integritätstest / Testen der Datenwiederherstellung

- Nach dem Erstellen eines Sicherungsmediums erfolgt ein automatischer Integritätstest des Sicherungsmediums. Der Integritätstest erkennt fehlerhafte Sicherungsdatensätze. Wird ein Fehler festgestellt, wird die Datensicherung erneut durchgeführt.
- Wird eine neue Datenquelle eingerichtet, wird nach dem Erstellen der ersten Sicherungskopie eine Wiederherstellung der gesicherten Daten durchgeführt. In regelmäßigen Abständen wird die Wiederherstellung von Sicherungskopien wiederholt.
- Auf diese Weise wird sichergestellt, dass die Sicherungsmedien und die darauf befindlichen Sicherungssätze bei Bedarf zur Wiederherstellung verwendet werden können.

5.2. Rasche Wiederherstellbarkeit

Es ist zu gewährleisten, dass die Verfügbarkeit der personenbezogenen Daten und er Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann (Art. 32 Abs. 1 lit. c DSGVO)

Die rms GmbH hat folgendes Konzept zum Wiederanlauf der IT für drei Szenarien erstellt:

5.2.1. Verlust des Serverraums und der IT-Systeme der Niederlassung Berlin

- Die Produktivdaten der Serversysteme in Berlin werden über den Standort Frankfurt gesichert und stehen bei einem Verlust der IT Systeme der Niederlassung Berlin als Datensicherung zur Verfügung.
- Im Serverraum des 2. OG am Standort Frankfurt stehen Storage- und Serversysteme mit freien Kapazitäten zur Verfügung, mit denen ein temporärer Betrieb der ausgefallenen IT Systeme ermöglicht wird. Aus der vorhandenen Datensicherung können die ausgefallenen IT Systeme wiederhergestellt werden und auf den Storage- und Serversystemen im 2. OG bis zum Eintreffen neuer Hardware am Standort Berlin betrieben werden.

5.2.2. Verlust des Serverraums und der IT-Systeme des 4.OG in Frankfurt

- Die Produktivdaten der Serversysteme des 4. OG werden über IT Systeme im 2. OG gesichert und stehen bei einem Verlust der IT Systeme des 4.OG als Datensicherung zur Verfügung. Die Serverräume im 2. und 4. OG befinden sich in unterschiedlichen Brandabschnitten des Gebäudes.
- Wie im vorangegangenen Szenario ermöglichen die im Serverraum des 2. OG am Standort Frankfurt stehenden Storage- und Serversysteme mit freien Kapazitäten einen temporären Betrieb der wichtigen IT Systeme des 4. OG. Aus der vorhandenen Datensicherung können die ausgefallenen IT Systeme wiederhergestellt werden und auf den Storage- und Serversystemen im 2. OG bis zum Eintreffen neuer Hardware für den Serverraum des 4. OG betrieben werden.
- Für 2018/2019 ist es vorgesehen, Leitungsinfrastruktur zur Anbindung an das Internet im Serverraum des 2. OG zu implementieren, um bei einem Totalausfall der Leitungsinfrastruktur im 4. OG umgehend alternative Verbindungen zum Internet herstellen zu können.

5.2.3. Verlust aller Serverräume und IT-Systeme

- Bei Verlust sämtlicher IT Systeme steht zunächst keine Hardware für den Betrieb der ausgefallenen IT Systeme zur Verfügung. Eine Neuanschaffung der zerstörten Hardware muss umgehend eingeleitet werden. Bis zum Eintreffen der neuen Hardware kann ein Notfallbetrieb in einem externen Rechenzentrum eingerichtet werden. Hierbei werden die wichtigsten IT Systeme aus den ausgelagerten Sicherungsmedien wiederhergestellt. Ein Zugriff auf die IT Systeme kann der Geschäftsführung und den Mitarbeitern über ein abgesichertes VPN zur Verfügung gestellt werden.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Der Verantwortliche implementiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (siehe Art. 32 Abs. 1 lit. d DSGVO)

Das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen bei der rms GmbH umfasst die folgenden Maßnahmen:

- Erstellung und Aktualisierung einer Übersicht über die ergriffenen technischen und organisatorischen Maßnahmen
- Führen eines Verzeichnisses aller Verarbeitungstätigkeiten, die der eigenen Zuständigkeit unterliegen
- Führen eines Verzeichnisses zu allen Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung
- Prüfungen durch den Datenschutzbeauftragten
- Regelmäßige Stichprobenkontrollen
- Anlassbezogene Kontrollen

7. Revisionsfähigkeit/Weisungsgemäße Verarbeitung

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) (§ 64 Abs. 3 Nr. 13 BDSG (neu))

7.1. Sicherstellung der weisungsgemäßen Verarbeitung durch eigene Mitarbeiter

Die rms GmbH ergreift folgende Maßnahmen, um sicherzustellen, dass personenbezogenen Daten, die im Auftrag verarbeitet werden, von den Mitarbeitern nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Verpflichtung der Beschäftigten auf Einhaltung des Datenschutzes
- Verpflichtung, die personenbezogenen Daten nur auf Weisung des Vorgesetzten zu verarbeiten

7.2. Auftragskontrolle

Die rms GmbH ergreift folgende Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, von Unterauftragnehmern nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Abschließen eines schriftlichen Vertrags mit Sub-Unternehmern bei Auftragsverarbeitung (AV-Vertrag) mit den gesetzlichen Mindestinhalten sowie darüberhinausgehenden Informationen zur genauen Auftragsgestaltung.
- Eindeutige Vertragsgestaltung
- Kontrollen der Sub-Unternehmen
- Regelung der Rechte und Pflichten des Auftraggebers und -nehmers im AV-Vertrag
- Regelung der technischen und organisatorischen Maßnahmen der Sub-Unternehmer im AV-Vertrag
- Zugänglichmachung des AV-Vertrags und der Weisungen für die involvierten Beschäftigten
- Trennung der Daten verschiedener Mandanten
- Vollständige Löschung der Daten nach Auftragsabschluss und Datenübergabe
- Schulung der Mitarbeiter zu den Anforderungen an den Datenschutz in Auftragsverarbeitungsverhältnissen
- Abstimmung unpräziser oder unklarer Weisungen
- Stichprobenkontrollen über die Einhaltung der Weisungen durch Mitarbeiter

RHEIN-MAIN-VERKEHRSVERBUND

Beschreibung vHGS

Anlage 11 zum vHGS-Vertrag

Thema:	Beschreibung vHGS
Dateiname:	19-02-20 Anlage 11 Beschreibung vHGS.doc
Erstellt am:	20.02.2019
Zuletzt geändert am:	20.02.2019
Version:	1.0
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV/rms	20.02.2019	Version als Anlage zum vHGS-Vertrag V1.1

Organisation und Datenverarbeitung im vHGS

1. Zweck des vHGS, Zweck der Verarbeitung

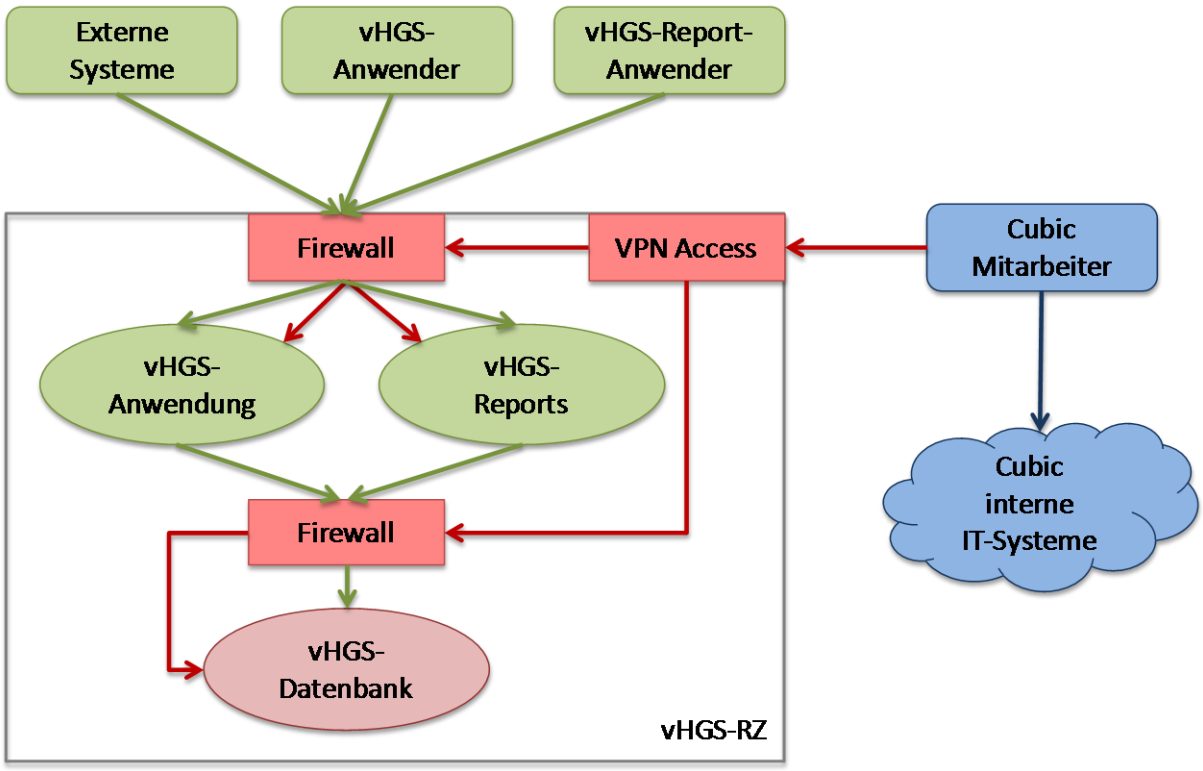
Das verbundweite, mandantenfähige Hintergrundsystem des RMV, kurz vHGS genannt, stellt ein Vertriebssystem für die Ausgabe und Verwaltung von Fahrkarten des öffentlichen Personennahverkehrs dar. Es unterstützt sowohl den direkten Vertrieb am „Point Of Sales“ in großen und kleinen Vertriebstellen als auch die Bearbeitung von Bestellungen und anderen Kundenwünschen in einem Backoffice. Neben der Bearbeitung von Kundenaufträgen, die über Bestellscheine eintreffen, werden auch die notwendigen Prozesse für die Bearbeitung von Aufträgen aus dem RMV-TicketShop bzw. aus dem RMV-Internetkundenportal meinRMV bereitgestellt, sowie für die Bearbeitung von elektronischen Auftragsdateien zu Sammelverträgen mit allgemeinen Großkunden, Nutzern des Firmenkundenrabats, Schulwegkostenträgern und JobTicket-Unternehmen.

Der RMV hat 2012 mit dem eTicket RheinMain die Ausgabe von Zeitkarten auf Chipkarten begonnen. Das eTicket RheinMain ist der Name für ein Verfahren, dass sich zur Ausgabe von RMV-Fahrkarten des zum Einführungszeitpunkt neuartigen Kernapplikationsstandards des Vereins Deutscher Verkehrsunternehmen (kurz VDV-KA) bedient. Da zum Einführungszeitpunkt kein Vertriebssystem eines RMV-Vertriebspartners in der Lage war, diesen Standard zu unterstützen, hatte sich der RMV dazu entschlossen, ein entsprechendes Vertriebssystem bereitzustellen und seinen Vertriebspartnern optional die Nutzung dieser gemeinsamen Vertriebsplattform anzubieten. Eine Ertüchtigung jedes einzelnen Vertriebssystems im Verbund konnte damit vermieden werden und darüber hinaus die Möglichkeit geschaffen werden, dass die beteiligten Vertriebspartner sich direkt gegenseitig vertrieblich im sog. „Service durch Dritte“ unterstützen können. Nur 3 von 41 Verkehrsunternehmen mit Vertriebsstellen im RMV betreiben eigene KA-fähige Vertriebssysteme.

Im Sinne des VDV-KA Standards deckt das vHGS im Hintergrund die klassischen Vertriebsfunktionen sowie den verpflichtenden KA-Datenaustausch von Kundenvertragspartner (KVP), Dienstleistern oder besser den kontrollierenden Verkehrsunternehmen (DL) und dem Produktverantwortlichen (PL) zwischen verschiedenen Akteuren des KA-Rollenmodells ab. Auch bzw. insbesondere, wenn sich einer der Akteure eines eigenen Vertriebssystem bedient.

2. Aufbau und Zugriff auf das vHGS

Die nachfolgende Abbildung zeigt eine Übersicht über den Aufbau und die Organisation des vHGS in Bezug auf den Zugang zum System:



Das vHGS wird zentral in einem Rechenzentrum (vHGS-RZ) betrieben und ist als Webanwendung für unterschiedliche Nutzergruppen erreichbar:

- Die vHGS-Anwender sind Mitarbeiter der Verkehrsunternehmen oder von diesen beauftragte Dienstleister, die in einer Vertriebsstelle oder in einem Backoffice Fahrkarten ausstellen, Kundenwünsche bearbeiten oder sonstige Aufgaben der Vertragsverwaltung erledigen.

- Die vHGS-Report-Anwender sind Mitarbeiter der Verkehrsunternehmen oder von diesen beauftragte Dienstleister, die die spezifischen Schnittstellen für die Übernahme der Buchungs- und Vertriebsdaten in die Finanzbuchhaltung ihrer Unternehmen erzeugen oder zur Meldung der Verkaufsdaten an ihre LNO bzw. den RMV. Andere Reports werden für vertriebliche Zwecke, wie die Provisionierung von Vertriebsstellen, erzeugt oder zur Bereitstellung von Managementinformationen bzw. Statistiken.

- Externe Systeme sind Terminalmanagementsysteme von Busdruckern, Kontrollgeräten und Automaten oder auch das RMV-Kundenportal **meinRMV** mit dem **RMV-TicketShop**. Darüber hinaus gehören aber auch KA-konforme Vertriebssysteme von Verkehrsunternehmen, die sich nicht des vHGS bedienen, jedoch über eine bidirektionale Schnittstelle (BIDI) mit dem vHGS verbunden sind, dazu. Im Weiteren auch die Systeme der **RMV-Bezahlplattform**, des Massenpersonalisierers, von Informationsdiensten oder Inkassounternehmen.

- Die Mitarbeiter des Systemherstellers und –betreibers **Cubic** haben darüber hinaus einen VPN-Zugang, der nicht nur die Nutzung der Applikation, sondern auch einen direkten Zugriff auf die Datenbank des vHGS zum Zwecke der Betriebsführung ermöglicht.

Das vHGS wurde unter Berücksichtigung der Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen entwickelt. Es gewährleistet im Rahmen der konkreten Auftragsverarbeitung ein dem Risiko angemessenes Schutzniveau

hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit durch die nachstehend aufgeführten Datenverarbeitungsprozesse und –maßnahmen. Die Entwicklung aller wesentlichen Teile des vHGS (u.a. Datenbankmodell, Prozesse, …) wurde zu Beginn umfassend durch den hessischen Datenschutzbeauftragten begleitet.

Die Zugriffsrechte werden im vHGS wie folgt organisiert:
Jeder Mandant im vHGS benennt einen Mitarbeiter als internen vHGS-Administrator. Dieser erhält von der technischen Betriebsführung des vHGS Zugangsdaten, die auf die Daten des entsprechenden Kundenvertragspartners bzw. der entsprechenden Kontrollorganisation beschränkt sind. Alle weiteren Mitarbeiter des Mandanten erhalten ihre Zugangsdaten von diesem internen Administrator. Dabei kann der Administrator maximal die eigenen Rechte vererben.

3. Datenerhebung, Datenbearbeitung

Die Bearbeitung von personenbezogenen Daten im vHGS berücksichtigt in jeder Phase die Grundsätze des Art. 5 DS-GVO. Hierzu gehören insbesondere

- die Zweckbindung der Daten,
- die Datenminimierung,
- die Speicherbegrenzung sowie
- die Integrität und Vertraulichkeit.

a) Mandantenspezifische Trennung der Daten in der gemeinsamen vHGS Datenbank

Alle Daten, die durch die Mandanten als Kundenvertragspartner oder Kontrollorganisation bzw. durch den Kunden selbstbedient über meinRMV in das vHGS eingegeben werden, werden in einer gemeinsamen Datenbank (ein Datenbankmanagementsystem) mit einem einheitlichen Datenmodel abgelegt.
Die mandantenspezifische Trennung der Daten (logische Datentrennung), die den Zugriff eines Mandanten in der Applikation eindeutig beschränkt, erfolgt entsprechend dem jeweiligen funktionalen Kontext über die folgenden Objekte:

- **Chipkarte**: Kundenvertragspartner können auf die Daten zugreifen, die mit der von ihnen ausgegebenen Chipkarte (über KA-Applikations-ID) verknüpft sind.

- **Fahrkarte**: Kundenvertragspartner können auf die Daten zugreifen, die mit den von ihnen verkauften Fahrkarten (über Berechtigungs-IDs) verknüpft sind.

- **Vertrag (Einzel- oder Sammelvertrag):** Kundenvertragspartner können auf die Daten zugreifen, die mit den von ihnen abgeschlossenen Einzel- oder Sammelverträge (über Name, Kunden-/Vertragsnummern) verknüpft sind.

- **Kontrollterminal**: Kontrollorganisationen können auf die Daten zugreifen, die sie über die TerminalManagementSchnittstelle (TMS) vom Hintergrundsystem ihrer Kontrollterminals an das vHGS geliefert haben (Verknüpfung über Geräte-ID).

Zur Optimierung des Kundenservice wurden Ausnahmen von der mandantenspezifischen Trennung der Daten in Einzelfällen möglich gemacht. Den sogenannten „Service durch Dritte“ kann ein Kunde in allen Vertriebsstellen des RMV in Anspruch nehmen und sich somit ggf. den Gang zu seinem Kundenvertragspartner ersparen.
Voraussetzung für den Zugriff auf Daten, die über die logische Grenze des jeweiligen Mandanten hinausgehen, bedarf der Zustimmung des Kunden im jeweiligen Einzelfall.

Der jeweilige Vertriebsmitarbeiter erhält immer einen Hinweis in Form eines PopUps, bevor er den „Service durch Dritte“ beginnt. Er kann nur weiterarbeiten, wenn er diesen Hinweis aktiv bestätigt. Diese Bestätigung durch den Mitarbeiter wird protokolliert.
Für externe Mandaten (RMV-Vertriebspartner mit eigenem KA-Vertriebssystem) werden die Informationen, die im Rahmen des “Service durch Dritte“ zur Verfügung gestellt werden, über eine entsprechende Schnittstelle (BIDI „Verkauf & Service“) zur Verfügung gestellt.

Ausnahme/Anwendungsfall Nr. 1: „Kundensuche“

Kundendaten werden im vHGS nach Möglichkeit nicht redundant angelegt (Datensparsamkeit); Weder, wenn sie mehrere Geschäftsbeziehungen mit einem Mandanten haben, noch, wenn sie diese mit unterschiedlichen Mandanten im vHGS haben. D.h. bspw., dass ein Mitarbeiter bei der Vertragsanlage innerhalb der ganzen, gemeinsamen vHGS-Kundendatenbank suchen und einen eventuell bereits vorhandenen Kundendatensatz mit dem eigenen Geschäftsvorfall verknüpfen kann.

Um Missbrauch vorzubeugen, wurde mit den Vertretern des hessischen Datenschutzbeauftragten abgestimmt, dass in der Kundensuche mindestens der erste Buchstabe des Vornamens und die ersten 6 Buchstabens des Nachnamens bzw. der gesamte Nachname als Suchkriterium vorgegeben werden müssen.

Ausnahme/Anwendungsfall Nr. 2 „Service durch Dritte“

Kunden sollen die Möglichkeit erhalten, sich für bestimmte Servicefälle an alle Vertriebsstellen im gesamten RMV-Gebiet wenden zu können, und nicht nur an Vertriebsstellen ihres jeweiligen Vertragspartners. Im Zentrum stehen dabei der Ersatz einer Chipkarte mit allen dazugehörigen Fahrkarten und der Erhalt von Kundeninformationen bezüglich nachfolgender Fragestellungen:

- Was steht auf der Chipkarte bzw. welche Fahrkarten sind darauf gespeichert?
- An wen muss der Kunde sich wenden, wenn er ein Anliegen hat, dass nicht durch einen „fremden“ Vertriebspartner im Rahmen des Service durch Dritte bearbeitet werden kann?

b) <u>Erhebung Kundenstammdaten und Vertragsdaten</u>

Die Erfassung der Daten ist für die Abwicklung der Vertragsbeziehung unabdingbar. Daten werden nach dem Prinzip der Datensparsamkeit/Datenminimierung erhoben (Kundenstammdaten werden nur einmalig erhoben und nicht – wie bis vor einiger Zeit – mehrfach in verschiedenen Vertriebssystemen gespeichert.)

Die Erfassung von Daten eines Kunden erfolgt

- auf Grundlage eines ausgefüllten und unterschriebenen Bestellscheins eines Kunden oder eines entsprechenden Kundenschreibens (u. a. in einer Vertriebsstelle oder im Backoffice),
- auf Grundlage seiner eigenen Angaben, die er über meinRMV online eingegeben hat oder
- auf Grundlage einer Bestelldatei eines Großkunden (z.B. Schulwegkostenträger).

Kunden, die keinen Vertrag abschließen bzw. ihre persönlichen Daten nicht Preis geben möchten, können im RMV alternativ anonym Fahrkarten auf Chipkarten erwerben.

c) Erhebung von Mitarbeiterstammdaten bzw. Mitarbeiterstammdaten von Subunternehmern

Mitarbeiterstammdaten werden vom jeweiligen Administrator des Mandanten für alle Mitarbeiter, die mit dem vHGS arbeiten, erfasst. Darüber hinaus bekommt der Mitarbeiter einen Benutzernamen und ein Passwort, welches der Mitarbeiter beim ersten Anmelden ändern kann bzw. ändern muss (sofern der Mandant dies so im vHGS selbst einrichtet). Der Administrator kann dann zwar weiterhin das Benutzerkonto des Mitarbeiters einsehen, jedoch kann sich nur der jeweilige Mitarbeiter an einem Terminal anmelden (da nur er das neue Passwort kennt).

Mit der Eingabe eines Mitarbeiters werden die für ihn vorgesehenen Rechte durch den Administrator konfiguriert.

Die Erfassung der Mitarbeiterdaten ist notwendig,

- um den Bearbeiter von Vorgängen im vHGS zu dokumentieren sowie
- um Parameter abzuspeichern (z. B. Telefonnummer), die in Kundenbelegen automatisiert eingetragen werden.

d) Erhebung von personenbezogenen Daten von privaten Vertriebspartnern

Zum Zwecke der Auszahlung von Provisionen wird eine zur Vertriebsstelle gehörige Bankverbindung sowie Steuernummer + USt-ID-Nummer erfasst.

e) Erhebung Transaktionsnachweise (Nachweise zur Kontrolle, Ausgabe, Rücknahme, Sperrung und Entsperrung)

Rechtsgrundlage ist auch hier Artikel 6 Abs. 1 Buchstabe b) DSGVO.

Die Erfassung ist für die Funktionalität des eTicket RheinMain

- zur Manipulation- und Missbrauchsanalyse,
- zur frühzeitigen Erkennung von ggf. vorhandenen Fehlern im System (z. B. wird die hier erkannt, wenn Terminals zeitweise keine Sperr- und Aktionslisten abrufen) und
- zur Sicherung der Datenqualität (z. B. Erkennen, ob der aktuelle Tarif geladen ist)

zwingend notwendig.

Die Daten werden von den jeweiligen Kontroll- bzw. Vertriebsterminals an ihr jeweiliges Terminal-Hintergrundsystem übermittelt (WLAN, Mobilfunk oder im Einzelfall über einen externen Datenspeicher) und von dort an das vHGS geliefert (über gesicherte Web-Schnittstelle, teilweise zusätzlich via VPN-Tunnel).

f) Protokollierung Datenzugriff
Protokollierung der Zugriffe auf die Daten ist Teil des Datensicherungskonzeptes und trägt zur Wahrung der Integrität und Vertraulichkeit der Daten bei.

Protokolliert wird lediglich der vHGS User-Name und nicht der Klarname des zugreifenden Mitarbeiters. Eine Zuordnung des User-Namen zum Klarnamen ist lediglich dem Administrator bzw. dem Mitarbeiter selbst möglich.

4. Datenübermittlung an externe Systeme/Empfänger

a) Massenpersonalisierer (MP)
Aufgabe des Massenpersonalisierers ist es, für die Mandanten – auf Auftrag hin – Chipkarten für deren Kunden mit den entsprechenden Fahrberechtigungen zu „beschreiben“. Darüber hinaus erfolgt dann auch der Versand der Chipkarten zusammen mit einem Anschreiben an die Kunden.

Der Austausch der dafür relevanten Daten zwischen MP und vHGS erfolgt über eine entsprechende Schnittstelle.

Kategorien von Daten, die verarbeitet werden
- **Benutzerverwaltungsdaten**: Mitarbeiter von der verantwortlichen Stelle, Benutzeridentifikation
- **Endkundenstammdaten**: Name, Vorname, Geschlecht, Titel, Geburtsdatum, Adresse (Straße, Hausnummer, Postleitzahl, Ort), E-Mail-Adresse, Bankverbindung (IBAN, BIC, Name des Bankinstituts), Kundennummer, Vertragsnummer, Chipkartennummer, zugeordnete Rolle (Besteller, Bezahler, Benutzer der Fahrkarte).
- **Endkundennutzungsdaten**: Berechtigungs-ID, Tarifprodukt (Fahrkartenart), Vertragspartner (leistungserbringendes Verkehrsunternehmen), Verkaufsdatum, Verkaufsuhrzeit, Start und Ziel Tarifgebiet, Beginn und Ende Gültigkeit, Preis

b) Bonitätsauskunft
Im Rahmen der Bestellbearbeitung können auf gesonderte Anfrage die personenbezogenen Daten Name, Geburtsdatum, Anschrift des Bestellers sowie die Daten zur Bankverbindung an eine festgelegte Auskunftei übermittelt zwecks Erhalts einer Bonitätsaussage.
Das Ergebnis der Bonitätsprüfung wird in Form einer Ampel angezeigt. Zudem besteht die Möglichkeit, sich darüber hinaus die konkreten Negativ-Merkmale anzeigen zu lassen.

Da ggf. jede einzelne Abfrage beim Auskunftsdienst kostenpflichtig ist, speichert das vHGS die Abfrageergebnisse. Wurde für einen Kunden bereits eine Auskunft eingeholt, wird nach Klicken auf den Button „Abfragen“ zunächst das Ergebnis dieser Abfrage angezeigt. Zu erkennen ist dies am Abfragedatum, das ggf. in der Vergangenheit liegt. Soll die Abfrage aktualisiert werden, also eine Bonitätsprüfung zum aktuellen n Datum durchgeführt werden, muss der Mitarbeiter auf „Abfrage aktualisieren“ klicken. Es wird dann eine weitere ggf. kostenpflichtige Auskunft für diesen Kunden eingeholt.

c) Geldinstitute, Kreditkartenunternehmen, Inkassounternehmen
Über die RMV-Bezahlplattform werden Zahlungen abgewickelt, die durch den Verkauf von RMV-Tickets für den öffentlichen Nahverkehr im Gebiet des RMV abzurechnen sind. Im Rahmen der Abrechnung werden die dafür erforderlichen personenbezogenen Daten an Geldinstitute, Kreditkartenunternehmen und Inkassounternehmen übermittelt. Ziel ist die Realisierung des mit dem Kunden vertraglich vereinbarten Geldeinzugs über Geldinstitute oder Kreditkartenunternehmen bzw. die Übergabe aller für ein gerichtliches Mahnverfahren notwendigen Daten an ein Inkassounternehmen.
Der Datenaustausch mit Hausbanken erfolgt über das EBICS-Verfahren.

Kategorien von Daten, die verarbeitet werden
- **Benutzerverwaltungsdaten**: Mitarbeiter von der verantwortlichen Stelle, Benutzeridentifikation, Benutzerstammdaten in Übereinstimmung mit der Hauptverwaltung, Benutzerverwaltung der Anwendung

- **Endkundenstammdaten**: Kontoinhaber (Vorname und Nachname), Kontodaten, Bank- oder Kreditkarteninformationen (Kreditkarteninhaber, Kreditkartenunternehmen (Visa/MasterCard) und Pseudokreditkartennummer [ReferenzID]), SEPA-Mandat
- **Endkundennutzungsdaten**: Kontoauszugsdaten des Verkehrsunternehmens, SEPA-Lastschriftinformationen, Buchungsdaten und Zahlungsinformationen Reporting, Transaktionsstatistik

5. Löschen von Daten, Löschfristen

Grundsätzlich gilt für alle gespeicherten Daten das Prinzip der Datensparsamkeit. Das bedeutet zum einen, dass nur die Daten erhoben werden dürfen, die unbedingt für die Ausführung des Dienstes notwendig sind. Zum anderen heißt das aber auch, dass die Daten nur so lange wie nötig im System vorgehalten werden dürfen.
Alle vom vHGS gespeicherten Daten werden einer Kategorie zugeordnet. Die folgende Tabelle führt die Kategorien auf, erläutert, warum sie erhoben werden, und spezifiziert, wie und wann sie wieder entfernt werden.

Kategorie	Datenart	Datenelemente	Grund der Datenhaltung	Behandlung/ Verfahren	Frist
LOGGING	Teils Dateien in Textform (Logfiles), teils Datenbankeinträge (Access Log)	Detaillierte Beschreibungen der Verarbeitungsschritte und evtl. auftretender Fehlersituationen.	Technische Problemlösung Sicherheitsanalysen	Löschung nach definierter Frist.	3 Monate
VERKAUF	Datenbank-einträge	Detaildatensätze der Verkaufstransaktionen	Nachweise entsprechend AGB/ABB, Grundlage der Rechnungsstellung	Löschung nach definierter Frist	Fallabschluss + 6 Monate
KUNDE	Datenbank-einträge	Detaildaten (Name, Adresse, …) zur Person des Kunden	Nachweise entsprechend AGB/ABB, Grundlage der Rechnungsstellung	Löschung nach definierter Frist	Fallabschluss + 6 Monate
FINANZ	Datenbankeinträge	Verträge (Abo, …)	Grundlage der Rechnungsstellung, Ausweis gegenüber Steuerbehörde	Löschung nach definierter Frist, nach Archivierung aufbewahrungspflichtiger Daten	Fallabschluss + 6 Monate Archiv Vertragsdaten: 10 Jahre
	Datenbank-einträge	Rechnungen und Bezahltransaktionen	Ausweis gegenüber Steuerbehörde	Löschung nach definierter Frist, nach Archivierung aufbewahrungspflichtiger Daten	Fallabschluss + 6 Monate Archiv Rechnungsdaten: 10 Jahre
	Datenbank-einträge	Sortennachweise (enthalten keine Kundendaten)	Ausweis gegenüber Wirtschaftsprüfer Statistik	Löschung nach definierter Frist	10 Jahre
SPERR-LISTEN	Datenbank-einträge	Kartennummern, Fahrkarten, die aufgrund einer Regelverletzung ausgeschlossen wurden	Schutz der Unternehmen vor Einnahmeausfällen.	Löschung nach definierter Frist	Fallabschluss + 3 Monate
KONTROLLE	Datenbank-einträge	Daten von Kontroll- und Sperrnachweisen	Sperrmanagement Auswertungen für Betrugsverdachtsanalyse	Analyse der Daten und anschließend Löschung	min. 3 Tage, max. 14 Tage

Hinweis zu Daten aus der Kontrolle von eTickets

In den bei der Kontrolle von eTickets entstehenden KA-Transaktionsnachweisen vom Typ TXEBER (059) werden bei Eingang im vHGS folgende Felder des Datenbereichs „AllgemeineFahrttransaktionsdaten“ mit „0“ (oder anderslautenden nichtinformationstragenden Werten) überschrieben:

- fahrtNummer
- berLogLinieVarianteID.linieID
- berLogLinieVarianteID.varianteNummer

6. Allgemeine im vHGS enthaltene technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

Zugangskontrolle
Die Anmeldung zum vHGS ist nur mit Benutzer ID und Kennwort möglich. Nach mehreren fehlgeschlagenen Anmeldeversuchen wird der Zugriff gesperrt. Die Passwörter werden als Hash-Werte abgelegt und können auch von Administratoren ausgelesen werden.

Zugriffskontrolle
Die Zugriffskontrolle erfolgt durch ein Benutzer- und Rollenkonzept: Nur nach Anmeldung mit Benutzername und Kennwort kann ein Zugriff auf die Daten erfolgen. Aktionen sind nur gemäß der jeweils individuellen Berechtigung des Benutzers möglich. Die Anzahl der Benutzer wird so klein wie möglich gehalten.

Weitergabekontrolle
Unbefugtes Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten wird durch Verschlüsselung und weitere Sicherheitsmaßnahmen entsprechend dem Stand der Technik verhindert. Die Schnittstellen des Systems sind klar definiert und entsprechend dem Stand der Technik gesichert.

Eingabekontrolle
Alle Änderungen und Weitergaben von Daten werden im System dokumentiert.

Auftragskontrolle
Die im Rahmen des vHGS von Dienstleistern übernommene Auftragsverarbeitung erfolgt ausschließlich auf Grundlage der DS-GVO sowie der jeweils mit dem Verantwortlichen getroffenen Vereinbarung zur Auftragsverarbeitung.

Verfügbarkeitskontrolle
Die personenbezogenen Daten sind mehrfach vor Verlust und Zerstörung gesichert. Zu den Sicherungsmaßnahmen gehören u.a. redundante Datenhaltung sowie eine regelmäßige Datensicherung.

Verpflichtung auf den Datenschutz
Alle Mitarbeiter werden während ihrer Tätigkeit mit dem vHGS und darüber hinaus zur Vertraulichkeit sowie auf die Einhaltung der Datenschutzrichtlinien hingewiesen und verpflichtet.

7. Wahrung der Rechte der Betroffenen

a) Erteilung von Auskünften und Einsichtnahme (gem. Art 15 DS-GVO)

Ein Betroffener kann sich bei seinem bzw. einem seiner Kundenvertragspartner (KVP) eine Auskunft über die von ihm im vHGS gespeicherten personenbezogenen Daten geben lassen. Diese Information beinhaltet ggf. auch KVP-übergreifend alle personenbezogenen, im vHGS gespeicherten Daten des Betroffenen.

Zur Vermeidung von Missbrauch wird diese Auskunft niemals direkt erteilt, sondern kann ausschließlich über den jeweiligen Datenschutzbeauftragten eines KVP beantragt werden.
Die Beantragung dieser Auskunft kann wie folgt erfolgen:

- Schriftlich,
- Per E-Mail an den jeweiligen Datenschutzbeauftragten des KVP,
- Persönlich in einer Vertriebsstelle (wobei die Vertriebsstelle verpflichtet ist, eine Identitätsprüfung durchzuführen und den Antrag erst dann an den entsprechenden Datenschutzbeauftragten weiterzuleiten).

Die Antwort erfolgt in den beiden ersten Fällen ausschließlich an die im vHGS gespeicherte Adresse bzw. E-Mail Adresse des Betroffenen, um sicher zu stellen, dass nicht ggf. ein Unberechtigter sich eine Auskunft über einen Dritten geben lässt.

Die Auskunft wird innerhalb von spätestens 4 Wochen schriftlich oder per E-Mail erteilt.

b) Benachrichtigungen

Daten werden ausschließlich mit Zustimmung der Betroffenen erhoben, daher entfallen Benachrichtigungen.

c) Datenberichtigung, –löschung gem. Art. 16 + 17 DS-GVO

Die Kundendaten können jederzeit auf Wunsch des Kunden korrigiert oder gelöscht werden, sofern weder gesetzliche Regelungen noch berechtigte Interessen des Verantwortlichen dagegen stehen.
Der Kunde bekommt nach der Änderung einen Beleg über die Änderung ausgehändigt.

d) Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO
Nicht relevant, da keine Möglichkeit zur Vertragsübernahme durch einen anderen Anbieter gegeben ist.

8. Risiko durch Datenmissbrauch

a) Verlust der Vertraulichkeit
Durch Abhören der Kommunikation: Daten, die während der Kommunikation mit dem System verschickt werden, werden von unberechtigten Personen mitgelesen.

Durch Auslesen der Datenbankinhalte: Innerhalb des Systems gespeicherte Daten werden von unberechtigten Personen ausgelesen. Systemadministratoren ist dies prinzipiell möglich. Nutzer können nur Daten in definierten Anwendungsfällen auslesen. Außenstehenden ist kein direkter Zugriff auf die Datenbankinhalte möglich sein.

Schutzmaßnahmen:
Die Kommunikation mit dem Webfrontend erfolgt über das https-Protokoll.
Die Kommunikation zwischen Terminalgeräten und Hintergrundsystem erfolgt ebenfalls über das https-Protokoll.
Firewalls etc. verhindern das Auslesen der Datenbank von außen.
Die Administratoren werden auf das Datenschutzgesetz verpflichtet.
Das Benutzerrollenkonzept regelt die Sicht auf personenbezogene Daten.
Die Anmeldung im System ist nur mit Benutzer-ID und Kennwort möglich.
Nach mehreren fehlgeschlagenen Anmeldeversuchen wird der Zugriff gesperrt.
Passwörter werden als Hash-Werte abgelegt und können auch von Administratoren nicht ausgelesen werden.
Der Datenaustausch mit Hausbanken erfolgt über das EBICS-Verfahren.

b) Verlust der Integrität
Durch Wiedereinspielen alter Transaktionsdaten: Dieser Angriff kann meist nur von den Administratoren des Systems durchgeführt werden, da diese als Einzige Zugriff auf alte Datenbankzustände haben.

Durch Maskerade: Der Angreifer ersetzt einen Kommunikationsteilnehmer und übernimmt dessen Rolle. Dadurch wird nicht nur die Vertraulichkeit verletzt, sondern auch die Zurechenbarkeit der Daten.

Durch Inkonsistenz gespeicherter Daten: Falls die Datenbank nicht in einem konsistenten Zustand gehalten wird, z.B. durch nicht-atomar ausgeführte Transaktionen, können Fehler und Datenverluste die Folge sein.

Durch Veränderung der Kommunikationsdaten: Durch einen Angreifer oder einen Systemfehler werden Manipulationen an den ausgetauschten Daten vorgenommen. Dies kann eine gezielte inhaltliche Änderung der Daten zur Folge haben oder einen Systemabsturz durch nicht interpretierbare Daten.

Schutzmaßnahmen:
Inkonsistenzen werden durch ACID-Prinzip verhindert (Transaktionen werden nur vollständig oder gar nicht durchgeführt).
Datenaustausch zwischen Terminals und Hintergrundsystem durch eine Ende-zu-Ende-MAC Sicherung gestützt.

c) Verlust der Verfügbarkeit
Durch Denial of Service (Sabotage): Durch gezielte Überlastung eines Servers wird versucht, den Dienst oder Teile davon arbeitsunfähig zu machen.

Durch Systemausfall: Bei einem Systemausfall können keine Transaktionen durchgeführt werden. Gründe können ein Angriff auf das System, Konfigurationsfehler oder ein Netzausfall sein.

Durch Verlust gespeicherter Daten: Falls Daten gelöscht oder verändert werden, können zahlreiche Transaktionen nicht mehr korrekt durchgeführt werden (z.B. Anmeldung, Bezahlvorgänge). Gründe für den Verlust können ein Angriff oder Fehler bei der Handhabung der Daten durch die Systemadministratoren sein.

Schutzmaßnahmen:
Die Server sind so konfiguriert, dass nur wirklich benötigte Funktionen verfügbar sind. Nicht benötigte Funktionen sind deaktiviert.
Maßnahmen zur Redundanz, Monitoring und automatisiertem Wiederanlaufen sind vorgesehen.

Folgende Tabelle zeigt exemplarisch mögliche Probleme im Zusammenhang mit den o.g. Risikofaktoren:

Vorgang	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
Anmeldung	Benutzerrelevante Informationen werden Unberechtigten bekannt.	Anmeldedaten werden auf dem Kommunikationsweg oder beim Speichern geändert	System nicht verfügbar
Kaufvorgang	Transaktionen werden offengelegt	Preise oder Transaktionsdaten werden manipuliert	System nicht verfügbar

Bezahlabwicklung	Unbefugte erhalten Kenntnis über Bezahldaten und Abbuchungsbeträge	Bezahlaufträge werden geändert (z.B. Kontonummer, Betrag)	System nicht verfügbar
Statistiken, Reporting	Unbefugte erhalten Informationen über Kundengewohnheit und können Profile erstellen	Statistiken werden gefälscht	System nicht verfügbar
Kundenservice	Unberechtigte erfahren z.B. von Zahlungsproblemen eines Kunden		Kein Kundenservice möglich
Kontrollnachweis	Durch unberechtigte Nutzung der Kontrollnachweise können anhand der enthaltenen eTicket-Kennungen Bewegungsprofile der Kunden erstellt werden		

RHEIN-MAIN-VERKEHRSVERBUND

Weisungsberechtigte

Anlage 12 zum vHGS-Vertrag

Thema:	Weisungsberechtigte
Dateiname:	19-02-20 Anlage 11 Beschreibung vHGS.doc
Erstellt am:	20.02.2019
Zuletzt geändert am:	20.02.2019
Version:	1.0
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	20.02.2019	Version als Anlage zum vHGS-Vertrag V1.1

Weisungsempfänger beim AN

- Herr Thomas Kern
  Geschäftsbereichsleiter Marketing, Vertrieb und Innovation,
  Telefon: 06192-294-400,

- Herr Walter Noé
  Bereichsleiter Vertrieb,
  Telefon: 06192-294-430 und

- Frau Christine Wierach
  Teamleiterin Vertrieb,
  Telefon: 06192-294-441.

Für Weisungen zu nutzende Kommunikationskanäle:

Rhein-Main-Verkehrsverbund GmbH
Alte Bleiche 5
65719 Hofheim/Ts.
E-Mail: vHGS_Auftragsverarbeitung@rmv.de

Weisungsberechtigte beim AG

Teilnehmer	Weisungsberechtigte

RHEIN-MAIN-VERKEHRSVERBUND

Subunternehmer des RMV

Liste mit Subunternehmern des RMV

Thema:	Liste mit Subunternehmen des RMV zum vHGS
Dateiname:	Liste Subunternehmer RMV
Erstellt am:	08.12.2011
Zuletzt geändert am:	20.02.2019
Version:	1.4
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
1.0	RMV	08.12.2011	Nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste enthält die vom RMV im Rahmen des vHGS eingesetzten Subunternehmer.
1.1	RMV	29.04.2014	Aktualisierte nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste enthält die vom RMV im Rahmen des vHGS eingesetzten Subunternehmer.
1.2	RMV	08.09.2016	Aktualisierte nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste enthält die vom RMV im Rahmen des vHGS eingesetzten Subunternehmer.
1.3	RMV	27.09.2017	Aktualisierte nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste enthält die vom RMV im Rahmen des vHGS eingesetzten Subunternehmer.
1.4	RMV/rms	20.02.2019	Aktualisierte nachrichtliche Anlage zum vHGS-Vertrag V1.1. Die Liste enthält die vom RMV im Rahmen des vHGS eingesetzten Unterauftragnehmer und (Unter-)Unterauftragnehmer.

Der RMV setzt zur Erfüllung seiner Leistungen im Rahmen des verbundweiten Hintergrundsystems (vHGS) des eTicket RheinMain die folgenden Subunternehmer ein:

TCS Cards & Services GmbH (ehemals Swiss Post Solutions GmbH)
Kronacher Straße 61
96052 Bamberg

Tel.: +49 (0)951 / 94 26 - 0
E-Mail: sales@tc-s.eu

Auftragsinhalt: Massenpersonalisierer

Umfang der Verarbeitung personenbezogener Daten:
Aufbringen von Kundenstammdaten auf Nutzermedien

Rhein-Main-Verkehrsverbund Servicegesellschaft mbH (rms GmbH)
Am Hauptbahnhof 6
60329 Frankfurt am Main

Tel.: Tel: 069-27307-555
Fax: 069-27307-477
E-Mail: vhgs.ufb@rms-consult.de

Auftragsinhalt: Betrieb der übergeordneten fachlichen Betriebsführung (üfB)

Umfang der Verarbeitung personenbezogener Daten:
keine

Weiterhin setzt die rms GmbH zur Erfüllung ihrer Leistungen im Rahmen des verbundweiten Hintergrundsystems (vHGS) des eTicket RheinMain die folgenden Subunternehmer ein:

Cubic Transportation Systems (Deutschland) GmbH
Alter Fischmarkt 11
20457 Hamburg

Tel.: 040-3008 6369-11
Fax: 040-30086369-10
E-Mail: vhgs.support@cubic.com

Auftragsinhalt:
Entwicklung und Betrieb des vHGS;
Betrieb der übergeordneten technischen Betriebsführung (ütB)

Umfang der Verarbeitung personenbezogener Daten:
Betrieb des vHGS in einem Rechenzentrum

RHEIN-MAIN-VERKEHRSVERBUND

Subunternehmer der Teilnehmer

Liste mit Subunternehmern der Teilnehmer am vHGS
mit Aufgabenbereich Online vHGS
(inkl. Service durch Dritte)

Thema:	Liste mit Subunternehmen der vHGS-Teilnehmer
Dateiname:	Liste Subunternehmer Teilnehmer
Erstellt am:	08.12.2011
Zuletzt geändert am:	06.06.2019
Version:	0.93
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
0.9	RMV	08.12.2011	Nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste der Subunternehmer der Teilnehmer enthält den Kenntnisstand zum 08.12.2011. Die abschließende Version 1.0 wird nach Abschluss der Vertragsunterzeichnungen nachgereicht.
0.91	RMV	29.10.2014	Laufende Aktualisierung neuer Mandanten und Namensänderung
0.92	RMV	22.08.2017	Laufende Aktualisierung neuer Mandanten und Namensänderung
0.93	RMV	06.06.2019	Laufende Aktualisierung neuer Mandanten und Namensänderung

Die Teilnehmer mit Aufgabenbereich Online vHGS (inkl. Service durch Dritte) setzen zur Erfüllung ihrer Leistungen die folgenden Subunternehmer ein:

Teilnehmer	**Eingesetzte(r) Subunternehmer**
ALV Marburg/Oberhessen GmbH & Co. oHG Ernst-Giller-Straße 7 35039 Marburg	keine
Becker & Sohn GmbH & Co. KG Am Bewegungsbad 1 35080 Bad Endbach	keine
Busverkehr Wissmüller GmbH Neutorstrasse 10 64720 Michelstadt	keine
DB Regio AG Region Hessen Mannheimer Straße 81 60327 Frankfurt am Main	DB Vertrieb GmbH Stephensonstr. 1 60326 Frankfurt am Main
Hanauer Straßenbahn GmbH Daimlerstr. 5 63450 Hanau	keine
Heuser Omnibusunternehmen GmbH & Co. KG Kinzigstraße 10 63505 Langenselbold	keine
HLB Basis AG Am Hauptbahnhof 18 60329 Frankfurt am Main	keine
Kreisverkehrsgesellschaft Main-Kinzig mbH Nürnberger Str. 41 63450 Hanau	keine
Kreis-Verkehrs-Gesellschaft Offenbach mbH Masayaplatz 1 63128 Dietzenbach	keine
LNVG Groß-Gerau Lokale Nahverkehrsgesellschaft mbH des Kreises Groß-Gerau Jahnstraße 1 64521 Groß-Gerau	keine
Lokale Nahverkehrsgesellschaft Fulda mbH Zieherser Weg 2 36037 Fulda	keine
Magistrat der Stadt Bad Homburg v.d.Höhe Rathausplatz 1 61348 Bad Homburg v.d.Höhe	HLB Basis AG Bahnstraße 13 61462 Königstein (Aboverwaltung)
Main-Taunus-Verkehrsgesellschaft mbH (MTV) Am Kreishaus 1-5 65719 Hofheim a. Taunus	keine
Offenbacher Verkehrsbetriebe GmbH (OVB) Hebestraße 14 63065 Offenbach	keine

Teilnehmer	Eingesetzte(r) Subunternehmer
Odenwald -Regional-Gesellschaft mbH (OREG) Marktplatz 1 64711 Erbach	keine
Regionalverkehr Main-Kinzig GmbH Barbarossastraße 26 63571 Gelnhausen	Keine
RDG Regionalverkehrsdienst Gründau Elke Laubach e.K. Brauhausweg 9 63584 Gründau	Keine
RNV Regionaler Nahverkehrsverband Marburg-Biedenkopf Im Lichtenholz 60 35043 Marburg	ALV Marburg/Oberhessen GmbH & Co. oHG Ernst-Giller-Straße 7 35039 Marburg Becker & Sohn GmbH & Co. KG Am Bewegungsbad 1 35080 Bad Endbach
RTV Rheingau-Taunus-Verkehrsgesellschaft mbH Heimbacher Straße 7 65307 Bad Schwalbach	Magistrat der Stadt Idstein König-Adolf-Platz 2 65510 Idstein (MobilitätsInfo)
Stadtlinienverkehr Limburg a.d. Lahn Hospitalstraße 2 65549 Limburg a. d. Lahn	keine
Stadtwerke Dietzenbach GmbH Thomas-Mann-Ring 2 - 4 63128 Dietzenbach	Kreis-Verkehrs-Gesellschaft Offenbach Masayaplatz 1 63128 Dietzenbach (Aboverwaltung)
Stadtwerke Gießen AG Lahnstraße 31 35398 Gießen	keine
Stadtwerke Langen GmbH Weserstraße 14 63225 Langen	Kreis-Verkehrs-Gesellschaft Offenbach Masayaplatz 1 63128 Dietzenbach (Aboverwaltung)
Stadtverkehr Maintal GmbH Berliner Straße 31 63477 Maintal	keine
Stadtwerke Marburg GmbH Am Krekel 55 35039 Marburg	keine
Stadtwerke Mühlheim am Main GmbH Dietesheimer Straße 70 63165 Mühlheim am Main	Kreis-Verkehrs-Gesellschaft Offenbach Masayaplatz 1 63128 Dietzenbach (Aboverwaltung)
Stadtwerke Neu-Isenburg GmbH Schleussnerstraße 62 63263 Neu-Isenburg	Kreis-Verkehrs-Gesellschaft Offenbach Masayaplatz 1 63128 Dietzenbach (Aboverwaltung)

Teilnehmer	**Eingesetzte(r) Subunternehmer**
Stadtwerke Oberursel (Taunus) GmbH Oberurseler Straße 55 - 57 61440 Oberursel (Taunus)	HLB Basis AG Bahnstraße 13 61462 Königstein (Aboverwaltung)
Stadtwerke Rodgau Friedberger Straße 37 63110 Rodgau	Kreis-Verkehrs-Gesellschaft Offenbach Masayaplatz 1 63128 Dietzenbach (Aboverwaltung)
RhönEnergie Fulda Bahnhofstraße 2 36037 Fulda	keine
RhönEnergie Bus GmbH Heinrichstraße 17/19 36037 Fulda	keine
traffiQ Lokale Nahverkehrsgesellschaft Frankfurt am Main mbH Stiftstr. 9-17 60313 Frankfurt am Main	Bewachungsinstitut Eufinger GmbH In der Römerstadt 52 60439 Frankfurt am Main
Verkehrsgesellschaft Lahn-Dill-Weil mbH Bahnhofstraße 14 35781 Weilburg	keine
Stadtwerke Verkehrsgesellschaft Frankfurt am Main mbH (VGF) Kurt-Schumacher-Straße 8 60311 Frankfurt am Main	keine
VGO Verkehrsgesellschaft Oberhessen mbH Hanauer Str. 15 61169 Friedberg	keine

RHEIN-MAIN-VERKEHRSVERBUND

Datenschutzbeauftragte der Teilnehmer

Liste mit Datenschutzbeauftragten
der Teilnehmer am vHGS
mit Aufgabenbereich Online vHGS
(inkl. Service durch Dritte)

Thema:	Liste mit Datenschutzbeauftragten der vHGS-Teilnehmer
Dateiname:	Liste Datenschutzbeauftragte Teilnehmer
Erstellt am:	08.12.2011
Zuletzt geändert am:	06.06.2019
Version:	1.1
Ersteller:	Rhein-Main-Verkehrsverbund GmbH

Versionsverwaltung

Version	Bearbeiter	Datum	Bemerkungen
0.9	RMV	08.12.2011	Nachrichtliche Anlage zum vHGS-Vertrag V1.0. Die Liste der Datenschutzbeauftragten der Teilnehmer enthält den Kenntnisstand zum 08.12.2011. Die abschließende Version 1.0 wird nach Abschluss der Vertragsunterzeichnungen nachgereicht.
1.0	RMV	18.08.2017	Die Liste der Datenschutzbeauftragten der Teilnehmer enthält den Kenntnisstand zum 18.18.2017.
1.1	RMV	06.06.2019	Die Liste der Datenschutzbeauftragten der Teilnehmer enthält den Kenntnisstand zum 06.06.2019.

Die Teilnehmer am vHGS mit Aufgabenbereich Online vHGS (inkl. Service durch Dritte) haben folgende Datenschutzbeauftragte benannt:

Teilnehmer	**Datenschutzbeauftragte(r)**
Busverkehr Wissmüller GmbH Neutorstrasse 10 64720 Michelstadt	Herr Karl Reinhard Wissmüller Wissmueller@wissmueller.de
DB Regio AG Region Hessen Mannheimer Straße 81 60327 Frankfurt am Main	Herr Chris Newiger chris.newiger@deutschebahn.com
Hanauer Straßenbahn GmbH Daimlerstr. 5 63450 Hanau	Frau Natalie Rudi natalie.rudi@hsb.de
HLB Basis AG Am Hauptbahnhof 18 60329 Frankfurt am Main	N.N.
Kreisverkehrsgesellschaft Main-Kinzig mbH Nürnberger Str. 41 63450 Hanau	Frau Carolin Böhm c.boehm@kvg-main-kinzig.de.
Kreis-Verkehrs-Gesellschaft Offenbach mbH Masayaplatz 1 63128 Dietzenbach	Frau Anette Heinemann ah@KVGOF.de
LNVG Groß-Gerau Lokale Nahverkehrsgesellschaft mbH des Kreises Groß-Gerau Jahnstraße 1 64521 Groß-Gerau	Herr Norbert Hartnick Norbert.Hartnick@LNVG-GG.de
Lokale Nahverkehrsgesellschaft Fulda mbH Zieherser Weg 2 36037 Fulda	N.N.
Magistrat der Stadt Bad Homburg v.d.Höhe Rathausplatz 1 61348 Bad Homburg v.d.Höhe	Ralf Gehrsitz Email: ralf.gehrsitz@bad-homburg.de Tel.: (06172)100-1500
Main-Taunus-Verkehrsgesellschaft mbH (MTV) Am Kreishaus 1-5 65719 Hofheim a. Taunus	N.N.
Mainzer Verkehrsgesellschaft mbH (MVG) Mozartstraße 8 55118 Mainz	Michael Schlömer Email: michael.schloemer@mvg-mainz.de Telefon: 06131/12-6354
Offenbacher Verkehrsbetriebe GmbH (OVB) Hebestraße 14 63065 Offenbach	Herr Patrick.Geinitz Patrick.Geinitz@OVB-OF.de Tel. (069) 80058305
Odenwald -Regional-Gesellschaft mbH (OREG) Marktplatz 1 64711 Erbach	Herr Moritz Görmann Email: m.goermann@ctm-com.de Tel.: (06154) 57605-0 (CTM-COM GmbH Wilhelm-Leuschner-Straße 33 64380 Roßdorf)
RTV Rheingau-Taunus-Verkehrsgesellschaft mbH Heimbacher Straße 7 65307 Bad Schwalbach	Herr Andreas Remler andreas.remler@rheingau-taunus.de Tel. (06124) 510-357

Teilnehmer	Datenschutzbeauftragte(r)
Stadtlinienverkehr Limburg a.d. Lahn Hospitalstraße 2 65549 Limburg a. d. Lahn	N.N.
Stadtwerke Dietzenbach GmbH Thomas-Mann-Ring 2 - 4 63128 Dietzenbach	N.N. (Stadtwerke Dietzenbach vertreiben keine Jahreskarten. Datenschutzbeauftragte(r) wird benannt, wenn CleverCards als eTicket vertrieben werden.
Stadtwerke Gießen AG Lahnstraße 31 35398 Gießen	N.N.
Stadtwerke Langen GmbH Weserstraße 14 63225 Langen	N.N.
Stadtwerke Marburg GmbH Am Krekel 55 35039 Marburg	Herr Lothar Goldbach Lothar.Goldbach@swmr.de
Stadtwerke Mühlheim am Main GmbH Dietesheimer Straße 70 63165 Mühlheim am Main	Herr Jürgen Hartz info@jhartz.de datenschutz@stadtwerke-muehlheim.de Tel.: 0172/6904696
Stadtwerke Neu-Isenburg GmbH Schleussnerstraße 62 63263 Neu-Isenburg	Herr Klaus Wenz k.wenz@swni.de Tel.: 06102/246330
Stadtwerke Oberursel (Taunus) GmbH Oberurseler Straße 55 - 57 61440 Oberursel (Taunus)	Frau Eva Simon Eva.Simon@Stadtwerke-Oberursel.de Tel. (06171) 509118
Stadtwerke Rodgau Friedberger Straße 37 63110 Rodgau	Frau Ingrid Sattler ingrid.sattler@rodgau.de 06106/82960
ÜWAG Überlandwerk Fulda Aktiengesellschaft Bahnhofstraße 2 36037 Fulda	Herr Hubert.Reinhardt Hubert.Reinhardt@Uewag.de Tel. (0661) 12340
ÜWAG Bus GmbH Heinrichstraße 17/19 36037 Fulda	Herr Hubert.Reinhardt Hubert.Reinhardt@Uewag.de Tel. (0661) 12340
Verkehrsgesellschaft Lahn-Dill-Weil mbH Bahnhofstraße 14 35781 Weilburg	N.N.
Stadtwerke Verkehrsgesellschaft Frankfurt am Main mbH (VGF) Kurt-Schumacher-Straße 8 60311 Frankfurt am Main	Herr Dirk Müller datenschutz@vgf-ffm.de Tel. 069 213-2 28 01
VGO Verkehrsgesellschaft Oberhessen mbH Hanauer Str. 15 61169 Friedberg	Herr Jens Schmidt Schmidt.J@OVAG.de Tel. (06031) 821271