Zusatzvereinbarung zum JET CARD VERTRAG

Vertrag über Auftragsverarbeitung im Sinne des Art. 28 DS-GVO

zwischen

JET Tankstellen Austria GmbH
Samergasse 27
5020 Salzburg-

- nachfolgend „**JET**" genannt

und

JET Card Kunde

- nachfolgend „**Auftraggeber**" genannt

Präambel

(A) Zwischen den Parteien besteht ein Flottenkartenvertrag (JET Card) (nachfolgend „**Basisvertrag**" genannt). Der vorliegende Auftragsverarbeitungsvertrag (nachfolgend der „**Vertrag**") findet Anwendung auf alle Datenverarbeitungstätigkeiten, die mit dem Basisvertrag in Zusammenhang stehen und bei denen JET, ihre Beschäftigten oder durch JET Beauftragte personenbezogene Daten im Auftrag des Auftraggebers verarbeiten.

(B) Unter diesem Vertrag handelt der Auftraggeber als Verantwortlicher i.S. der DS-GVO und JET als Auftragsverarbeiter im Rahmen einer Auftragsverarbeitung gem. § 28 DS-GVO.

1 Definitionen

1.1 **DS-GVO:** Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung).

1.2 **BDSG:** Bundesdatenschutzgesetz in der jeweils gültigen Fassung.

1.3 **Personenbezogene Daten**: Alle Informationen, die sich auf eine identifizierbare natürliche Person (nachfolgend: „**betroffene Person**" genannt) beziehen. Als identifizierbar ist eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4 **Besondere Kategorien von Daten**: Personenbezogene Daten, aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowiegenetische Daten, biometrische Daten, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung.

1.5 **Datenverarbeitung**: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die **Offenlegung** durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.6 Auftragsverarbeitung: **Auftragsverarbeitung ist die** Verarbeitung personenbezogener Daten durch JET im Auftrag von Auftraggeber.

2 Regelungsgegenstand

2.1. Gegenstand und Zweck der Datenverarbeitung

JET verarbeitet die in Ziffer 2 näher beschriebenen personenbezogene Daten im Auftrag des Auftraggebers und nach dessen dokumentierten Weisungen (Auftragsverarbeitung). Dies umfasst alle Datenverarbeitungstätigkeiten, die erforderlich sind, um die Leistungen zu erbringen, die Gegenstand des zwischen den Parteien bestehenden Basisvertrages sind. Hierbei verarbeitet JET die personenbezogenen Daten nur, soweit dies zur Erbringung der im Basisvertrag beschriebenen Serviceleistungen notwendig ist.

2.2. Dauer der Verarbeitung

Die Datenverarbeitung darf nur solange erfolgen, wie sie für die Durchführung der mit dem Auftraggeber im Basisvertrag vereinbarten Leistungen notwendig und gemäß den datenschutzrechtlichen Regelungenzulässig ist. Nach Abschluss der Erbringung der Verarbeitungsleistungen müssen alle personenbezogenen Daten nach Wahl Auftraggebers entweder gelöscht oder zurückgegeben und bestehende Kopien vernichtet werden, sofern nicht nach dem Unionsrecht oder aufgrund von Gesetzen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Erteilt der Auftraggeber nach Abschluss der Erbringung der Verarbeitungsleistungen keine Weisung, werden die Daten gelöscht.

Die vom Auftraggeber erteilten dokumentierten Weisungen hinsichtlich der Dauer der Verarbeitung sind zu befolgen.

2.3. Art der Datenverarbeitung:

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DS-GVO und des BDSG soweit dies für die Durchführung der mit dem Auftraggeber im Basisvertrag vereinbarten Leistungen erforderlich ist. Die vom Auftraggeber erteilten dokumentierten Weisungen hinsichtlich der Art der Verarbeitung sind zu befolgen. JET verarbeitet die personenbezogenen Daten nur, soweit es für die Durchführung der mit dem Auftraggeber im Basisvertrag vereinbarten Leistungen erforderlich ist. Die Einschaltung von weiteren Auftragsverarbeitern ist nur unter den in Ziffer 6 geregelten Voraussetzungen zulässig.

Findet die Datenverarbeitung nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, ist die Verlagerung in ein Drittland nur zulässig, wenn die besonderen Voraussetzungen der Artt. 44 f DS-GVO erfüllt sind.

2.4. Art der personenbezogenen Daten und die Kategorien der betroffenen Personen:

2.4.1. Art der personenbezogenen Daten:

Anschrift (Anrede, Vor- und Zunamen, Adresse), E-Mail-Adresse, Telefonnummer, Firmennamen inkl. Rechtsform, Handelsregisternummer und Umsatzsteuer-Identifikationsnummer, KFZ-Kennzeichen, Kilometerstände, Angaben zum monatlichen Umsatz/Absatz und zur Fahrzeuganzahl, Einkaufsvorgänge inklusive Ort, Uhrzeit und Angaben zu Warengruppen und Umsatz/Absatz, Angaben dazu, wie der JET Card Kunde auf JET aufmerksam geworden ist, ob der JET Card Kunde bereits andere Flottenkarten benutzen und wie der JET Card Kunde seine Vertragsunterlagen erhalten will, IP-Adresse, Art und Umfang der vom JET Card Kunden abgerufenen Elemente sowie Datum und Uhrzeit des Zugriffs.

2.4.2. Besondere Kategorien von Daten:

Es werden keine besonderen Kategorien von Daten verarbeitet.

2.4.3. Kategorien der betroffenen Personen:

JET Card Kunden, deren Mitarbeiter und anderen Fuhrparkberechtigten.

3. Pflichten von JET

3.1. JET darf Daten nur im Rahmen des Basisvertrages und der durch den Auftraggeber erfolgten dokumentierten Weisungen verarbeiten, es sei denn, es liegt ein Ausnahmefall im Sinn des Artikel 28 Abs. 3 lit. a DS-GVO vor. Die anfänglichen Weisungen ergeben sich aus dem Basisvertrag und dieser Vereinbarung; sie können vom Auftraggeber durch einzelne dokumentierte Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündlich erteilte Einzelweisungen sind vom Auftraggeber unverzüglich schriftlich oder in elektronischer Form zu bestätigen.

JET informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. JET darf die Weisung solange aussetzen, bis sie vom Auftraggeber in dokumentierter Form bestätigt oder abgeändert wird.

3.2. JET sichert in ihrem Verantwortungsbereich die Umsetzung und Einhaltung angemessener technischer und organisatorischer Maßnahmen zum Schutz der personenbezogenen Daten zu, die den besonderen Anforderungen des Datenschutzes gerecht werden (Art. 32 DS-GVO). Insbesondere wird JET technische und organisatorische Maßnahmen treffen, die (i) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen und sie im Falle eines physischen oder technischen Zwischenfalls rasch wiederzustellen und (ii) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen beinhalten. Die von JET zu treffenden Sicherungsmaßnahmen beinhalten insbesondere die in der Anlage 1 aufgeführten Maßnahmen.

JET ist berechtigt, die getroffenen Sicherheitsmaßnahmen zu ändern, hierbei muss JET jedoch sicherstellen, dass das vertraglich vereinbarte und gesetzlich vorgesehene Schutzniveau nicht unterschritten wird. Auf Anfrage stellt JET dem Auftraggeber ein aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. JET ist verpflichtet, ihre Sicherungsmaßnahmen laufend zu überprüfen und erforderlichenfalls dem technischen Fortschritt anzupassen. Bei Verstößen gegen diese Verpflichtung ist JET verpflichtet, diese unverzüglich zu beseitigen.

JET unterstützt den Auftraggeber im Rahmen ihrer Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte und bei der Einhaltung der in Artt. 32 bis 36 DS-GVO genannten Pflichten. JET stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung.

Wendet sich eine betroffene Person mit Anträgen auf Berichtigung, Löschung oder Auskunft an JET, wird JET die Anfrage unverzüglich an den Auftraggeber zur Beantwortung durch den Auftraggeber weiterleiten; JET wird den Auftraggeber hierbei angemessen unterstützen.

3.3. JET gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Vertraulichkeitspflicht unterliegen.

3.4. JET ist verpflichtet Überprüfungen - einschließlich Inspektionen - durch die zuständigen Datenschutzbehörden, den Auftraggeber oder vom Auftraggeber beauftragte Dritte, sofern diese nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten zu ermöglichen und dazu beizutragen. Der Auftraggeber wird Überprüfungen nur im erforderlichen Umfang durchführen und die Betriebsabläufe von JET dabei nicht unverhältnismäßig stören.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber ist verpflichtet, JET unverzüglich und vollständig zu unterrichten, wenn der Auftraggeber in den Auftragsergebnissen Fehler oder Unzulänglichkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

4.2. Der Auftraggeber ist verpflichtet, JET die Kontaktdaten des betrieblichen Datenschutzbeauftragten mitzuteilen, sofern ein betrieblicher Datenschutzbeauftragter bestellt wurde.

5. Inanspruchnahme durch betroffene Personen hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO

5.1. Sollte eine der Parteien von einer betroffenen Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO in Anspruch genommen werden, verpflichtet sich die andere Partei, die in Anspruch genommene Partei bei der Abwehr der Ansprüche im Rahmen ihrer Möglichkeiten zu unterstützen.

6. Weitere Auftragsverarbeiter

6.1. Unter der Bedingung, dass der Unterauftrag schriftlich oder in einem elektronischen Format als Auftragsverarbeitung ausgestalten ist oder die Datenverarbeitung auf Grundlage eines anderen Rechtsinstruments im Sinne von Art. 28 Abs.3 DS-GVO erfolgt und den Anforderungen und Regelungen dieses Vertrages und der einschlägigen Gesetze, insbesondere der DS-GVO, entspricht, stimmt der Auftraggeber der Beauftragung der in der Anlage 2 aufgeführten weiteren Auftragsverarbeiter (Unterauftragnehmer) zu.

6.2. Der Auftraggeber stimmt zu, dass JET weitere Auftragsverarbeiter hinzuzieht, wenn der Unterauftrag den Regelungen in Absatz 1 entspricht. JET ist jedoch verpflichtet den Auftraggeber vor der Hinzuziehung von weiteren Auftragsverarbeitern zu informieren. Der Auftraggeber ist berechtigt, der Hinzuziehung aus wichtigem Grund zu widersprechen. Erfolgt innerhalb von 2 Wochen nach Zugang der Information kein Widerspruch, gilt die Zustimmung zur Hinzuziehung als erteilt. Im Falle eines Widerspruchs ist JET berechtigt die Leistung ohne die beabsichtigte Hinzuziehung weiterer Auftragsverarbeiter zu erbringen oder den Basisvertrag außerordentlich zu kündigen.

7. Laufzeit und Kündigung

7.1. Dieser Vertrag wird auf unbestimmte Zeit abgeschlossen. Er endet, ohne dass es einer Kündigung bedarf, automatisch mit der Beendigung des Basisvertrages. Eine isolierte ordentliche Kündigung dieser Vereinbarung ist ausgeschlossen. Das Recht auf Kündigung aus wichtigem Grund bleibt unberührt.

7.2. Mit Beendigung dieses Vertrages aus welchem Grund auch immer hat JET sämtliche bei ihr oder einem etwaigen Subunternehmer verbleibende personenbezogene Daten datenschutzgerecht zu löschen bzw. deren Löschung zu veranlassen, sofern nicht nach dem Unionsrecht oder aufgrund von Gesetzen eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Auf Verlangen des Auftraggebers wird JET alle in ihrem Besitz oder im Besitz eines etwaigen Subunternehmers befindlichen personenbezogenen Daten zurückzugeben. Soweit personenbezogene Daten nach Vertragsbeendigung im Besitz von JET oder eines etwaigen Subunternehmers verbleiben, gelten die Regelungen dieser Vereinbarung auch nach deren Beendigung für diese Daten fort.

8. Sonstiges

8.1. Sollten eine oder mehrere Bestimmungen dieses Vertrages unwirksam und/oder undurchführbar sein oder werden, bleibt die Wirksamkeit des übrigen Vertrages hiervon unberührt. Die ungültige Bestimmung ist durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, wenn sie bei Abschluss des Vertrags an die Ungültigkeit des jeweiligen Punktes gedacht hätten. Soweit diese Vereinbarung eine unbewusste Regelungslücke enthält, ist diese durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, wenn sie bei Abschluss des Vertrags an die Regelungsbedürftigkeit des jeweiligen Punktes gedacht hätten. Hierbei ist zu berücksichtigen, dass sich der Vertrag nach den Regelungen der DS-GVO und des BDSG in der jeweils gültigen Fassung richtet. Ungültige und fehlende Regelungen sind daher entsprechend der Vorgaben der DS-GVO und des BDSG zu ersetzen.

8.2. Es gilt deutsches Recht. Zwischen Kaufleuten ist Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag das Amtsgericht Hamburg Mitte; bei Überschreitung der gesetzlichen Streitwertgrenze das Landgericht Hamburg.

Anhang 1 - Technische und organisatorische Maßnahmen nach Art. 32, Abs. 1 DSGVO für die Nutzung von JET Card

1 Inhalt

2. Dokumentenklassifizierung

Die Informationen in diesem Dokument sind nach JET / Phillips66 Standards mit ‚Internal Only' klassifiziert. Das bedeutet, dass Sie mit Vertragspartner von JET oder Phillips66 ausgetauscht werden können. Eine Veröffentlichung, z.B.in Printmedien oder im Internet ist nicht zulässig. Eine Weitergabe an Dritte, die nicht Vertragspartner von JET sind, ist ebenfalls nicht zulässig, sofern es nicht um eine Anforderung zuständiger Aufsichtsbehörden handelt.

3. Vertraulichkeit

3.1 Zutrittskontrolle

Die Datenverarbeitung findet in Rechenzentren der JET Tankstellen Austria GmbH, JET Tankstellen Deutschland GmbH, der Phillips 66 Company in den USA und in Rechenzentren von Drittanbietern statt. Alle Rechenzentren erfüllen aktuelle Sicherheitsnormen.
Alle Rechenzentren sind als Sicherheitsbereiche konzipiert und mit elektronischen Zutrittskontrollsystemen gesichert. Sämtliche Zutritte werden protokolliert. Im Falle eines Ausfalls des elektronischen Schließsystems ist ein Zutritt über Schlüssel möglich. Die Verwaltung der Schlüssel unterliegt denselben Richtlinien wie bei den Zutrittskarten.
Der Zutritt zu den Rechenzentren wird nur Personen gewährt, die diesen im Rahmen Ihrer Aufgaben benötigen. Management of Change Prozesse stellen sicher, dass nicht mehr benötigte Zutrittsberechtigungen entzogen werden.
Betriebsfremde Personen, z.B. Dienstleister, die Zutritt zu den Rechenzentren benötigen, müssen sich am Empfang anmelden und halten sich nicht unbeaufsichtigt in den Datenverarbeitungsräumen auf.
Büroräume sind ebenfalls durch ein Zutrittskontrollsystem gesichert. Besucher müssen sich am Empfang anmelden und erhalten dort einen Besucherausweis. Sämtliche Besuche werden protokolliert. Darüber hinaus gilt eine Ausweispflicht für Mitarbeiter und Besucher. Alle Mitarbeiter sind darauf geschult, Personen, die allein und ohne Ausweis in den Räumlichkeiten angetroffen werden, anzusprechen und zum Empfang zu begleiten.
Die Rechenzentren sind größtenteils alarmgesichert und werden von Leitständen überwacht.

3.2 Zugangskontrolle

Die Vergabe von Zugängen erfolgt nach dem Least-Access-Prinzip. Mitarbeiter und Dienstleister erhalten nur den Zugang zu Systemen, den sie für ihre Arbeit benötigen.
Die Verwaltung von Zugängen erfolgt über zentrale Verzeichnisdienste. Zugangsberechtigungen sind immer personenbezogen, eine Ausnahme stellen Benutzeraccounts für die Kommunikation der Systeme untereinander dar. Richtlinien untersagen die Verwendung solcher Accounts für die interaktive Anmeldung von Benutzern.
Zugänge werden über ein Rechte- und Rollenkonzept gesteuert. Es erfolgt eine regelmäßige Überprüfung der zugeteilten Rollen und Rechte. Management of Change Prozesse stellen sicher, dass nicht mehr benötigte Zugangsberechtigungen entzogen werden.
Administrative Zugänge sind von normalen Benutzeraccounts getrennt und verfügen über eingeschränkte Kommunikationsrechte, z.B. E-Mail und Internet.

Administrative Tätigkeiten über externe Verbindungen erfolgen entweder über VPN, Zscaler oder separat gesicherte Extranet-Portale und immer gemäß aktueller Technik verschlüsselt. Darüber hinaus ist ein zweiter Faktor zur Authentifizierung erforderlich.

Alle Passwörter unterliegen aktuellen Regeln zur Passwortkomplexität und haben nur eine begrenzte Gültigkeit. Eine Speicherung von Passwörtern im Klartext oder eine Weitergabe an andere Benutzer ist durch die Benutzerrichtlinien untersagt. Passwörter können nicht regelmäßig wiederverwendet werden.

Nach mehrmaliger Fehleingabe des Passwortes erfolgt eine Sperrung des Benutzerkontos. Benutzerkonten, die innerhalb eines definierten Zeitraums nicht genutzt werden, werden automatisch gesperrt und nach Ablauf einer weiteren Frist gelöscht.

Zugänge zu anderen Netzen sowie zum Internet sind über Firewalls abgesichert. Darüber hinaus kommen Intrusion Detection und Prevention Systeme zu Einsatz, die schadhaften Datenverkehr erkennen und blockieren.

3.3 Zugriffskontrolle

Benutzerkonzepte stellen sicher, dass Benutzer nur auf die Daten zugreifen können, die sie für ihre Arbeit benötigen. Alle Zugriffe werden protokolliert.

Durch entsprechende Testkonzepte ist sichergestellt, dass die systemseitige Umsetzung der Benutzerberechtigungen auch nach Software-Anpassungen noch voll funktionsfähig ist.

Alle Benutzer müssen bei Verlassen des Arbeitsplatzes ihre Workstation sperren, die Vorgaben dazu sind in der Benutzerrichtlinie geregelt. Zudem sperrt sich die Workstation nach einigen Minuten der Inaktivität selbst.
Dokumente werden durch Druckersysteme nicht direkt ausgeworfen, sondern sind durch eine individuelle PIN am Drucker geschützt, welche vor dem Ausdruck eingegeben werden muss.

Es ist sichergestellt, dass Daten, die zu Testzwecken verwendet werden, denselben Zugriffsberechtigungen unterliegen wie in der Produktionsumgebung.

Sofern sich Kundendaten auf mobilen Endgeräten oder Datenträgern befinden, werden diese bei der Speicherung verschlüsselt. Ein Mobil Device Management stellt sicher, dass die Daten auf verlorengegangen Geräten aus der Ferne gelöscht werden können. Mitarbeiter sind angewiesen, Verlust oder Diebstahl solcher Geräte umgehend zu melden.

Es ist über die Benutzerrichtlinien untersagt, Unternehmens- und Kundendaten auf privaten Endgeräten zu speichern und zu verarbeiten.

Sofern Datenträger vernichtet werden müssen, erfolgt dies über zertifizierte Dienstleister mit entsprechender Protokollierung.

3.4 Trennbarkeit

In den Systemen für die JET Card werden nur Daten für die dazugehörigen Prozesse verarbeitet. Alle Daten sind anhand der Kunden- bzw. Debitorennummer sowie der Benutzerkennung eindeutig zuzuordnen. Diese Zuordnung wird in allen Transaktionen gewährleistet. Kunden haben keinen Zugriff auf Daten anderer Kunden.

Durch entsprechende Testkonzepte ist sichergestellt, dass die systemseitige Umsetzung der Kundentrennung auch nach Software-Anpassungen noch voll funktionsfähig ist.

3.5 Pseudonymisierung / Anonymisierung

Die verarbeiteten Daten werden - soweit notwendig - entsprechend der gesetzlichen Aufbewahrungsfristen gespeichert. Soweit ein Personenbezug notwendig ist, bliebt dieser über die gesamte Aufbewahrungszeit bestehen.

Sofern Daten nur für statistische Zwecke erhoben werden, wird geprüft und festgelegt, wann eine Anonymisierung möglich ist.

Bei einer Übertragung an Dienstleister oder zwischen Systemkomponenten ist sichergestellt, dass nur die Daten übertragen werden, die vom Empfängersystem zur Verarbeitung benötigt werden.

4. Integrität

4.1 Weitergabekontrolle

Im Rahmen der Auftragsverarbeitung werden nur Mitarbeiter und Dienstleister eingesetzt, die mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht wurden und die sowohl für die Zeit ihrer Tätigkeit als auch nach Beendigung des Beschäftigungsverhältnisses zur Verschwiegenheit verpflichtet sind.

Die Verarbeitung der Daten erfolgt ausschließlich in Rechenzentren. Es kommen Firewall-Technologien und Netzwerksegmentierungen zum Einsatz, um die Daten gegen Eingriffe von außen abzusichern.

Bei einer Übertragung von Daten an Dienstleister oder über das Internet werden die Daten nach dem aktuellen Stand der Technik verschlüsselt. Dies erfolgt i.d.R. über VPN oder verschlüsselte Webservices. Auch browserseitig wird eine Verschlüsselung über SSL nach aktuellem Stand der Technik eingesetzt.

Benutzerkennung und Passwort werden gesondert versendet. Das gleiche gilt auch für die Tankkarten und PINs. PIN-Briefe werden nach aktuellen Verfahren zur Sicherung der PIN und Erkennung von Missbrauch erstellt.

Eine Weitergabe der Daten erfolgt nur an autorisierte Dienstleister im Rahmen der vertraglich geregelten Zuständigkeiten. Es existieren ein Verzeichnis alle Datenverarbeitungen und Verträge mit entsprechenden Weisungen für Dienstleister. Datenübertragungen werden protokolliert

4.2 EingabekontroNe

Eingaben an Systemen können nur durch Mitarbeiter erfolgen, die aufgrund ihres Aufgabenbereichs Zugriff haben oder durch den Kunden selbst. Der Umfang der Berechtigungen wird durch eine Rollen- und Rechtematrix gewährleistet.

Der Kunde ist verantwortlich für die Vergabe von Berechtigungen innerhalb eines Kundenprofils und deren regelmäßige Überprüfung.

Alle Änderungen an Datensätzen sowie administrative Tätigkeiten werden protokolliert.

4.3 Auftragskontrolle

JET setzt nur Auftragnehmer ein, die ein entsprechendes Sicherheitsniveau garantieren können. Eine entsprechende Prüfung erfolgt bei Vertragsabschluss. Die Einhaltung und Aktualisierung des Sicherheitsniveaus kann durch regelmäßige Audits überprüft werden.

Eine Weitergabe der Daten erfolgt nur an autorisierte Dienstleister im Rahmen der vertraglich geregelten Zuständigkeiten. Es existieren ein Verzeichnis alle Datenverarbeitungen und Verträge mit entsprechenden Weisungen für Dienstleister.

Auftragsbezogene Weisungen werden dokumentiert.

5. Verfügbarkeit und Belastbarkeit

Die Rechenzentren verfügen über redundante Versorgungssysteme mit USV sowie Dieselgeneratoren. In den Rechenzentren werden ferner Brandfrüherkennungssysteme eingesetzt, die automatisch einen Löschvorgang auslösen können, wenn ein Brand erkannt wird. Darüber hinaus erfolgt eine Überwachung der Umweltkontrollen (Temperatur, Wasser) - entsprechende Abweichungen führen zu einer automatischen Alarmierung.

Die Server- und Technikräume sind vollständig klimatisiert.

Entsprechende Notfallpläne regeln die Abschaltung und Wiederherstellung von Systemen sowie das Wiederherstellung von Daten aus Back-ups. Diese Pläne werden regelmäßig getestet und aktualisiert.

Zum Schutz vor Datenverlust kommen entsprechende Datensicherungskonzepte zum Einsatz. Alle Daten werden entsprechend ihrer Kritikalität regelmäßig gesichert. Die Back-ups werden in der Regel in ein zweites Rechenzentrum überspielt. Eine Sicherung auf physikalische Datenträger erfolgt nicht.

Alle Systeme werden bezüglich ihrer Verfügbarkeit überwacht (Monitoring). Je nach Kritikalität erfolgt eine automatische Alarmierung des zuständigen IT-Personals im Falle eines Ausfalls.

Alle im Netzwerk betrieben Endgeräte und Server sind mit einem Virenschutz ausgestattet. Die Virusdefinitionen werden regelmäßig aktualisiert. Darüber hinaus wird durch Konzepte für Patches und Softwareaktualisierung dafür gesorgt, das Systeme immer mit aktuellen Sicherheitsmaßnahmen ausgestattet sind.

Durch regelmäßige Trainings und Awareness-Kampagnen werden Benutzer für IT- Sicherheit, zum Beispiel hinsichtlich Schadsoftware sensibilisiert. Darüber hinaus werden auch regelmäßig Schulungen zum Datenschutz durchgeführt.

6. Regelmäßige Überprüfung Bewertung und Evaluierung

JET Tankstellen Austria GmbH ist ein Unternehmen der Phillips66 Gruppe. Als solches unterliegt JET dem Phillips66 Information Security Management System (ISMS), dass auf den in DIN ISO/IEC 27001 und dem NIST Framework beschriebenen Maßnahmen basiert. Die vorliegend beschriebenen technischen und organisatorischen Maßnahmen sind wesentlicher Bestandteil dieses Systems.

Die Einhaltung der technischen und organisatorischen Maßnahmen werden im Rahmen des ISMS überwacht und durch interne und externe Audits überprüft, um so auch den Nachweis der Datensicherheit gewährleisten zu können.

Überprüfungsprozesse stellen sicher, dass das ISMS stets an den aktuellen Stand der Technik angepasst wird. Darüber hinaus regeln entsprechende Verfahren, die durch den Datenschutzbeauftragten überwacht werden, dass die getroffenen Maßnahmen hinsichtlich des Datenschutzes regelmäßig überprüft und an die aktuellen Anforderungen angepasst werden.

7. Maßnahmen zur Meldung von Datenschutzverstößen

JET verpflichtet sich, im Falle von Datenverstößen im Sinne von Art. 33 DSGVO diese unverzüglich und möglichst binnen 72 Stunden, nachdem JET die Datenschutzverletzung bekannt geworden ist, an den Verantwortlichen zu melden. Bei einer Meldung mehr als 72 Stunden nach Bekanntwerden des Datenschutzverstoßes, wird diese Verspätung begründet. JET trägt durch entsprechende Maßnahmen, wie u.a. Schulungen der Mitarbeiter und Mitarbeiterinnen, dafür Sorge, dass die etablierten Prozesse bekannt sind und im Fall eines Datenverstoßes angewendet werden. Durch das Einrichten entsprechender Meldeketten ist JET in der Lage, die Pflichten, die in Art 33 benannt sind, zu erfüllen.

Anhang 2 - Liste der Subunternehmer für JET Card Systeme

Subunternehmer	Erbrachte Dienstleistung	Rechtsgrundlage der Datenübermittlung
JET Tankstellen Deutschland GmbH Caffamacherreihe 1 20335 Hamburg	Systemmanagement und Support Weiterentwicklung	Auftragsverarbeitungs vertrag
CANCOM Managed Services GmbH Erika-Mann-Straße 69 80636 München	Hosting, PaaS Datenübertragung	Auftragsverarbeitungs vertrag
Phillips66 Company 2331 CityWest Blvd, Houston, TX 77042 USA	Hosting Datenübertragung Netzwerkbetrieb ERP	Standardvertrags klauseln
PAYONE GmbH Lyoner Straße 9 60528 Frankfurt/Main	Netzbetrieb	Auftragsverarbeitungs vertrag
dynamic4work GmbH Gründgensstraße 18 22309 Hamburg	Software-Entwicklung Wartung und Support	Auftragsverarbeitungs vertrag
KNISTR GmbH Hugh-Greene-Weg 2 22529 Hamburg	Autorisierung	Auftragsverarbeitungs vertrag
SPS Germany GmbH Delivery Document Output Kirchheimer Straße 177 73265 Dettingen u. Teck	Karten- und PINBrief-Produktion	Auftragsverarbeitungs vertrag
INTREXX GmbH Eugen-Martin-Str. 14 79106 Freiburg	SoftwareEntwicklung Wartung und Support	Auftragsverarbeitungs vertrag
Reinfeldt & Dr. Hellgardt Rechtsanwälte Eiffestraße 76 20537 Hamburg	Kunden ServiceCenter	Auftragsverarbeitungs vertrag
Microsoft Corporation Dept. 551, Volume Licensing 6100 Neil Road, Suite 210 Reno, Nevada 89511-1137 USA	E-Mail und Datenablage	Standardvertrags klauseln
Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 United States	Datenablage	Standardvertrags klauseln
Amazon Europe Marcel-Breuer-Straße 21 80807 München	Datenablage	Standardvertrags klauseln
Accenture International Limited 1 Grand Canal Square Grand Canal Harbour, Dublin 2, D02 P820.	ERP Support und Weiterentwicklung	Standardvertrags Klauseln
mit Betriebsstätten in Houston, TX, United States Pune, Mumbai, Bengaluru, Hyderabad, India Manila, Phillipines		

Versionskontrolle

Version	Datum	Autor	Freigegeben durch	Kommentare
1.0	25.06.2018	Anja Sonnenschein	Brigitte Götz Datenschutz-beauftragte	Erstversion
1.1	09.09.2018	Anja Sonnenschein		AVV Review - keine Änderungen notwendig
1.2	10.06.2020	Anja Sonnenschein		AVV Review - keine Änderungen notwendig Anhang 2 Review - Firmierungen angepasst
1.3	11.08.2021	Anja Sonnenschein		AVV Review - geringfügige Anpassungen Anhang 2 Review - Firmierungen / Adressen angepasst
1.4	07.06.2022	Anja Sonnenschein		 Anhang 1 Review - geringfügige Anpassungen (Zugangstechnologien) Anhang 2 Review - weitere Lieferanten hinzugefügt
1.5	21.03.2023	Anja Sonnenschein, Brigitte Götz		AVV Review - Punkt 7 Ergänzung Maßnahmen zur Meldung von Daten-schutzverstößen Anhang 2 Review - Weiteren Lieferanten hinzugefügt Anpassung Firmierungen, Ergänzung Datenschutz-grundlage
1.6	13.11.2023	Manuela Lechner		Anhang 2 Review - Anpassung Firmierungen