Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

§ 1 Allgemeines, Gegenstand und Dauer des Auftrags

1.1. Dieser Auftragsverarbeitungsvertrag (im Folgenden **„Vertrag"**) wird zwischen der S-Payment GmbH, Am Wallgraben 115, 70565 Stuttgart (Auftragsverarbeiter - nachstehend **„S-Payment", „Auftragnehmer"**) und Ihnen (Verantwortlicher - nachstehend **„Händler"**, **„Auftraggeber"**; [ggf.: Vertreter gemäß Art. 27 DSGVO]) abgeschlossen.

1.2. Der Gegenstand des Auftrags zum Datenumgang ergibt sich aus den Lizenz- und Nutzungsbedingungen zur Nutzung und Überlassung des in der Anwendung „Kartenakzeptanz" innerhalb der Sparkasse POS App angebundenen S-POS Plug-ins am Point of Sale.

1.3. Diese Lizenz- und Nutzungsbedingungen bringen es mit sich, dass der Auftragsverarbeiter personenbezogene Daten beim Einsatz des S-POS Plug-ins am Point of Sale in der App Hülle „Sparkasse POS" im Auftrag des Händlers (Auftraggebers) verarbeitet. Aus diesen Lizenz- und Nutzungsbedingungen ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

1.4. Die Dauer dieses Auftrags entspricht der Laufzeit der Lizenz- und Nutzungsbedingungen des S-POS Plug-ins.

§ 2 Umfang, Art und Zweck der Verarbeitung; Art der personenbezogenen Daten; Kategorien betroffener Personen

2.1. Umfang, Art und Zweck des Datenumgangs ergeben sich aus dem Kartenakzeptanzvertrag mit dem Netzbetreiber. Die Datenverarbeitung durch das S-POS Plug- in erfolgt insbesondere zu Zwecken der Übermittlung der personenbezogenen Daten durch das S-POS Plug-in zu den transaktionsabwickelnden Systemen des Netzbetreibers.

2.2. Betroffene Personen sind Kunden, die eine Zahlung am Point of Sale durchführen, deren Kartendaten durch das S-POS Plug-in ausgelesen werden.

2.3. Die Verarbeitung beginnt mit dem Einsatz zur Zahlungsakzeptanz am Point of Sale und endet mit der Übermittlung der personenbezogenen Daten an die transaktionsabwickelnden Systemen des Netzbetreibers zur weiteren Verarbeitung der Zahlungsabwicklung durch den Netzbetreiber. Die S-Payment speichert nach der Übermittlung keine personenbezogenen Daten die durch das S-POS Plug-in ausgelesen und übermittelt wurden.

2.4. Folgende personenbezogene Daten werden zur Übermittlung verarbeitet:

1. Erhebung & Verarbeitung personenbezogener Daten am POS:
    - Während des Bezahlvorgangs am POS wird der Karteninhabername ausgelesen. Dieser wird jedoch nicht gespeichert oder weitergeleitet
    - Es wird die PAN (Kartennummer) ausgelesen – diese wird für die weitere technische Verarbeitung der Transaktion benötigt.

§ 3 Technische und organisatorische Maßnahmen

3.1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Die technischen und organisatorischen Maßnahmen (TOM) des Auftragnehmers werden in diesem Fall durch die technischen und organisatorischen Maßnahmen eines Unterauftragnehmers ergänzt. Die Dokumentation der technischen und organisatorischen Maßnahmen (TOM) ist unter folgenden Links abrufbar: TOM des Auftragnehmers (S-Payment GmbH), TOM des Unterauftragnehmers (CCV GmbH).

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs.1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

3.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen

umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berechtigung, Einschränkung und Löschung von Daten

4.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nachdokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer verpflichtet sich zu einer schriftlichen Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Der Datenschutzbeauftragte ist wie folgt erreichbar:

   eMail: datenschutz@s-payment.de
   Telefon: 0711 782-21151

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung Ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

6.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachstehend „**Unterauftragnehmer**“) erbringen lassen.

6.2. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmer oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß AVV erbringt.

6.3. Der Auftragnehmer wird mit den Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen in Sinne dieser Regelungen sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§ 7 Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer oder ggf. mit dem Unterauftragnehmer (z.B. CCV GmbH), Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen . Hierbei hat der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) ein schlüssiges Datensicherheitskonzept (Auditzusammenfassung – Datenschutz der CCV GmbH), ggf. Zertifizierungen sowie Prüfberichte seiner externen Prüfer vorzulegen. Erachtet der Auftraggeber, nach der Prüfung des Datensicherheitskonzept und/oder der Prüfberichte das festgelegte Sicherheitsniveau als unzureichend , sind, soweit erforderlich, durch den Auftragnehmer oder ggf. den Unterauftragnehmer (CCV GmbH) ergänzende Maßnahmen umzusetzen. Der Auftraggeber hat bei der Umsetzung der erforderlichen Maßnahmen, die Aufgrund durch den Auftraggeber abgegebenen Beurteilung des Sicherheitsniveaus des Auftragsverarbeiters umzusetzen sind, durch liefern von Mängelberichten mitzuwirken.

7.2. Der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers oder ggf. des Unterauftragnehmers (CCV GmbH) nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO.

7.4. Für den Fall, dass konkrete Anhaltspunkte für Mängel und/oder Fehlverhalten bei der Verarbeitung personenbezogener Daten vorliegen und/oder begründete Zweifel an der Einhaltung der datenschutzrechtlichen Anforderung auftreten, kann der Auftraggeber weitere Informationen vom Auftragnehmer oder ggf. vom Unterauftragnehmer (CCV GmbH) verlangen. Wenn diese, vom Auftragnehmer oder ggf. vom Unterauftragnehmer (CCV GmbH) gelieferten weiteren Informationen nicht genügen, hat der Auftraggeber das Recht Vor-Ort-Prüfungen beim Auftragnehmer oder ggf. beim Unterauftragnehmer (CCV GmbH) durchzuführen. Die Vor-Ort-Prüfung kann durch den Auftraggeber nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden. Der Auftraggeber hat das Recht, maximal eine Vor-Ort-Prüfungen pro Jahr, bei Härtefällen jedoch auch mehrmals, innerhalb der üblichen Geschäftszeiten ohne Störung des Betriebslaufs durchzuführen.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
c) Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
d) Die Unterstützung des Auftraggebers für dessen ggfs. erforderliche Datenschutz-Folgenabschätzung.
e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers oder ggf. des Unterauftragnehmers (CCV GmbH) zurückzuführen sind, kann der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

9.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2. Der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschen und Rückgabe von personenbezogenen Daten

10.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung/Weisung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer oder ggf. der Unterauftragnehmer (CCV GmbH) entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.