Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

CCV Deutschland GmbH
Gewerbering 1
84072 Au i. d. Hallertau

(- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -)

und

POS-PARTNER

_____

_____

_____

(-Verantwortlicher - nachstehend Auftraggeber genannt -)

[ggf.: Vertreter gemäß Art. 27 DSGVO:

.....]

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer, wobei nicht zwingend alle aufgeführten Leistungen in Anspruch genommen werden:

1.1 Remote Verwaltung von Terminals

1.2 Nachbuchen von Zahlungen für Kunden im Fehlerfall

1.3 Bereitstellung und Betrieb eines App-basierten Kassensystems

1.4 Bereitstellung und Betrieb einer Online Plattform für Webshops

1.5 Bereitstellung und Betrieb eines Kundenportals „MyCCV“

1.6 Verwaltung von Geschenkkarten, Hosten der Geschenkkartendaten

1.7 Überprüfung, Reparatur oder Refurbishment von CCV Produkten

1.8 Bereitstellung Kundensupport

1.9 Bereitstellung eines Kundenportals für Transaktionsreporting

1.10 Verarbeitung von Transaktionen

1.11 Zahlungsabwicklung über Treuhandkonto

1.12 Werbeaktionen von CCV Marketing

1.13 Bereitstellung und Betrieb des „CCV Market Place“

1.14 Versand von postalischen Rechnungen

1.15 Open Application Manager: Entwicklung und Hosting paymentnaher Erweiterungsmodule

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Zu 1.1: Durchführung von Softwareupdates, wobei die Konfigurationsdaten und Logdateien der Terminals verarbeitet und im TKS bzw. TMS System gespeichert werden.

Zu 1.2: Von Kunden eingesendete Belege werden von Customer Service Direct Business manuell nachgebucht.

Zu 1.3: Bereitstellung eines Kassensystems, Hosten von Kunden- und Verbraucherstammdaten, Fernwartung, Einrichten des Kassensystems, Anlegen von Kundenstammdaten, Vor-Ort-Service, Zahlungsabwicklung über

Terminalanbindung, ggfs. MMS Verwaltung mit Meraki, Versand von Belegen an Verbraucher-E-Mail, Mitarbeiterverwaltung, Supportdienstleistung.

Zu 1.4: Bereitstellung eines Onlineshops, Anlage und Hosting von Kunden- und Kundenstammdaten, Fernwartung, Einrichten des Onlineshops, Zahlungsdienstleistung, Versand von Belegen an Verbraucher-E-Mail, Supportdienstleistung.

Zu 1.5: Plattform „MyCCV“ für CCV Kunden zur Verwaltung der CCV Produkte an zentraler Stelle. Zentrales Boarding für Kunden, Ermöglichung von Transaktions-Reports in einem DATEV-Format.

Zu 1.6: Mehrwertsystem, über das Verbrauchern Geschenkgutscheine verkauft werden kann und die Gutscheindaten verwaltet werden können.

Zu 1.7: Überprüfung, Reparatur oder Refurbishment von Hardware, Sicherung von Gerätedaten und Logdateien, Aktualisierung von Software.

Zu 1.8: Bearbeitung von Kundenanfragen bei technischen und kommerziellen Problemen und Wünschen. Bereitstellung einer Up- und Downloadplattform zum Datenaustausch. Bereitstellung eines Aktivierungscodes für den Einbau von Automatenterminals (4eye Tool).

Zu 1.9: Webservice mit Kundenlogin zur Überwachung der Transaktionsdaten.

Zu 1.10: Abwicklung von bargeldlosem Zahlungsverkehr in Terminals und Webshops.

Zu 1.11: Bündelung des Zahlungsverkehrs und Auszahlung über CCV Treuhandkonto inkl. Monitoring.

Zu 1.12: Versendung Newsletter, Prospektmaterial und Einladungen zu Veranstaltungen.

Zu 1.13: Geschlossener App Store „CCV Market Place“ zur Bereitstellung von CCV Produkten und 3rd Party Applikationen.

Zu 1.14: Herstellung und Beförderung von digital eingelieferten Sendungen mit klassischer Briefpost.

Zu 1.15: Funktionsbausteine können ergänzt werden, die den Leistungsumfang der Payment-Applikation erweitern. Die Funktionsbausteine werden entwickelt (OAM-Schnittstelle) und gehostet (OAM-Server).

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

Zu 1.1: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Terminal ID, IP-Adresse, Unterschrift des Verbrauchers

Zu 1.2: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Kartennummer, KFZ-Nummer, Kontonummer

Zu 1.3: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Telefon- und Faxnummer, E-Mail-Adresse, Steueridentifikationsnummer, Bankdaten, Artikeldaten, Unterschrift des Verbrauchers

Zu 1.4: Kunde: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Telefon- und Faxnummer, E-Mail-Adresse, IP-Adresse, Geburtsdatum; Verbraucher: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Telefon- und

Faxnummer, E-Mail-Adresse, IP-Adresse, Geburtsdatum, Bankverbindung, Bestellungen, Produkte & Dienstleistungen.

Zu 1.5: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Telefon- und Faxnummer, E-Mail-Adresse, IP-Adresse, Geburtsdatum, Vertragsabrechnungs- und Zahlungsdaten, Bankverbindung, Verbraucher Emailadresse, Verbrauchername, Personalausweis Kopie des Kunden, Handelsregisterauszug des Kunden, Umsatzsteuer-ID.

Zu 1.6: Kundendaten.

Zu 1.7: Personenstammdaten Kunden, Kontaktdaten Kunden, Bezahldaten Verbraucher, Personenstammdaten Endkunde, Fahrzeugdaten, Kommunikationsdaten Kasse, Standortdaten, Artikeldaten, Personenstammdaten Mitarbeiter, Kommunikationsdaten Kunden zu Backend und Kunde zu Backend, Artikeldaten, Artikelfotos, Kontodaten Kunden und Kunden.

Zu 1.8: Personenstammdaten Kunden, Kontaktdaten Kunden, Bezahldaten Verbraucher, Personenstammdaten Endkunde, Fahrzeugdaten, Kommunikationsdaten Kasse, Standortdaten, Artikeldaten, Personenstammdaten Mitarbeiter, Kommunikationsdaten Kunden zu Backend und Kunde zu Backend, Artikeldaten, Artikelfotos, Kontodaten Kunden und Kunden.

Zu 1.9: E-Mail-Adresse, Kundennummer, Terminal ID, VU Nummer.

Zu 1.10: Personenstammdaten Kunden, Bezahldaten Verbraucher, Personenstammdaten Endkunde, Fahrzeugdaten, Artikeldaten, Kontodaten Kunden und Kunden, Unterschriften, Kommunikationsdaten.

Zu 1.11: Anrede, Vor- und Nachname (ggf. Titel), E-Mail-Adresse, Telefon- und Faxnummer, Unterschrift, Zahlungsdaten (Umsatzdaten, Transaktionsdaten etc.), Vertragsabrechnungsdaten, Bankverbindung, Vertragspartnernummer, Vertragsdaten, Konfigurationsdaten der technischen Schnittstellen (IP-Adressen, PC-Konfigurationen etc.), Konfigurationsdaten zu Verwaltungsprogrammen sowie Online-Portalen, Personalausweiskopie des Kunden, Handelsregisterauszug des Kunden, Umsatzsteuer ID des Kunden.

Zu 1.12: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Position/Funktion, E-Mail-Adresse.

Zu 1.13: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Standortdaten.

Zu 1.14: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, Vertragsdaten, Vertragsabrechnungs- und Zahlungsverkehrsdaten, Position/Funktion, Mandatsnummer.

Zu 1.15: Anrede, Vor- und Nachname (ggf. Titel), Anschrift, E-Mail-Adresse, Telefonnummer, Faxnummer, Terminal ID, IP-Adresse, VU-Nummer, Unterschrift des Verbrauchers.

(3) Kategorien betroffener Personen

Die Kategorien, der durch die Verarbeitung betroffenen Personen, umfassen:

Zu 1.1: Kunde, Verbraucher

Zu 1.2: Kunden

Zu 1.3: Kunden, Interessenten

Zu 1.4: Kunden, Verbraucher

Zu 1.5: Kunden, Verbraucher

Zu 1.6: Kunden

Zu 1.7: Kunden, Verbraucher

Zu 1.8: Kunden, Verbraucher

Zu 1.9: Kunden

Zu 1.10: Kunden, Verbraucher

Zu 1.11: Kunden, Verbraucher

Zu 1.13: Kunden, Kooperationspartner

Zu 1.14: Kunden, Kooperationspartner

Zu 1.15: Kunden

Zu 1.16: Kunden, Verbraucher

3. Technisch-organisatorische Maßnahmen

(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. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(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 [Einzelheiten in Anlage 1].

(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. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter 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.

(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 Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

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

   eMail: datenschutz@de.ccv.eu

   Telefon: +49-8752 864 0

b) Die Wahrung der Vertraulichkeit gemäß Art. 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 Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

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 Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer Unterauftragnehmer (weitere Auftragsverarbeiter) zur Leistungserfüllung beauftragt. Mit Einschaltung weiterer Auftragsverarbeiter wird der Auftragnehmer zum Hauptauftragnehmer. Im Vorfeld einer Veränderung in Bezug auf die Einschaltung oder Ersetzung von Unterauftragnehmern wird der Auftragnehmer den Auftraggeber über diese Änderung informieren. Der Auftraggeber hat insoweit ein Einspruchsrecht. Der Hauptauftragnehmer ist verpflichtet, jedem Unterauftragnehmer ebenfalls die Pflichten aus diesem Auftragsverarbeitungsvertrag aufzuerlegen. Folgende Unterauftragnehmer verarbeiten derzeit relevante Daten:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
CCV Group B.V.	Westervoortsedijk 55 6827 Arnheim Niederlande	Betrieb der Backendsysteme für: 1.1 (nur TMS; TKS wird vom Auftragnehmer selbst betrieben), 1.3, 1.5, 1.6,1.10
BS Payone GmbH	Lyoner Straße 9 60528 Frankfurt Deutschland	Backendsysteme für: 1.2, 1.10
Samhammer AG	Zur Kesselschmiede 3 92637 Weiden Deutschland	Supportdienstleister für: 1.8
Volksbank in der Ortenau eG	Okenstraße 7 77652 Offenburg Deutschland	Bereitstellung Zwischenkonto für: 1.11
Continum AG	Bismarckallee 7b-d 79098 Freiburg Deutschland	Rechenzentrum für Backendsysteme für 1.10
Biedmeer B.V. (CCV Shop)	Diamantstraat 3 7554 TA Hengelo (Ov) Niederlande	Webshop zu 1.4
Deutsche Post ePost	Moltkestr. 14 53173 Bonn Deutschland	Versand von postalischen Rechnungen zu 1.14
CCV Lab BVBA	Spinnerijstraat 99 bus 12 8500 Kortrijk Belgien	Bereitstellung der Dienste zu 1.3, 1.5 und 1.6

Onslip Cloud AB	Kungsgatan 20 582 18 Linköping Schweden	Zu 1.3
The Rocket Science Group, LLC (MailChimp)	675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 US	Newsletterversand zu 1.12
COMPUS Computer GmbH	Max-Planck-Str. 4 85609 Aschheim-Dornach Deutschland	Reports DATEV-Format zu 1.5
Meraki LLC	500 Terry Francois Blvd. San Francisco, CA 94158 USA	Zu 1.3

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erhebt der Auftraggeber gegen die Einschaltung eines Unterauftragnehmers außerhalb der EU/des EWR keinen Einspruch, verpflichtet sich der Auftragnehmer, mit dem Unterauftragnehmer einen Vertrag über die EU-Standardvertragsklauseln abzuschließen. Anderenfalls ist eine Einschaltung von Unterauftragnehmern außerhalb der EU/des EWR unzulässig.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer im Falle vorheriger allgemeiner schriftlicher Genehmigung des Auftraggebers bedarf der vorherigen ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber, die über einen Tag hinausgehen, kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer 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.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

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

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

10. Löschung und Rückgabe von personenbezogenen Daten

(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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung/Weisung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer 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.

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

Au i.d. Hallertau, _____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift, Auftragnehmer	Stempel, Unterschrift, Auftraggeber

Anlage 1 – Technisch-organisatorische Maßnahmen

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

Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

- Elektronisches Schließsystem (Chipkarten)
- Schlüsselregelung
- Alarmanlage
- Besucherregelung mit Protokollierung
- Tragepflicht von Berechtigungsausweisen
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

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

- Zuordnung von Benutzerrechten
- Verwendung von sicheren Kennwörtern mit Ablaufzeit
- Erzwingen von automatischen Sperrmechanismen und Komplexitätsanforderungen
- Sperren von externen Schnittstellen (USB usw.)
- Einsatz von Anti-Viren-Software
- Einsatz von VPN-Technologie

Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge und Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Berechtigungskonzept
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Pseudonymisierung und Verschlüsselung

(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) Wird nach gesetzlichen Vorgaben oder auf Verlangen Betroffener oder Auftraggeber durchgeführt und protokolliert. Verschlüsselung wird bei mobilen Datenträgern eingesetzt.

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

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Ausschließlich verschlüsselte Datenübertragungswege werden verwendet
- Ausschließlich verschlüsselte Datenträger werden verwendet
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung

Eingabekontrolle

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

- Eingaben erfolgen teilweise automatisiert, eine manuelle Bearbeitung der Daten ist dann nicht vorgesehen
- Einsatz von Protokollierungsmechanismen wie Dokumentenmanagement- und Ticketsystem
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Automatische Löschanlage in Serverräumen
- Vorhandenes Backup- und Recoverykonzept
- Notfallplan
- Serverraum nicht unter sanitären Anlagen

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)

Maßnahmen, die gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird.

- Vorhandenes Backup- und Recoverykonzept
- Cold Standby Systeme
- Schattenkopien

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

Datenschutz-Management

Maßnahmen, die gewährleisten, dass Anforderungen der DSGVO nachprüfbar umgesetzt werden.

- Regelmäßige Datenschutz Audits
- Interne Revision
- Jährliche Mitarbeiter Datenschutz Schulungen

Incident-Response-Management

Maßnahmen, die gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern seine Daten betroffen sind.

- Bereitstellung von Infos über ContactCenter

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Maßnahmen, die gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden.

- Manuelle Softwareunterstützung
- Manuelle Löschung nach gesetzlicher Vorgabe
- Manuelle Löschung auf Anforderung

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Daten werden nicht ohne konkreten Auftrag verarbeitet
- Schriftliche Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Sorgfältige Auswahl von Unterauftragnehmern
- Vereinbarungen zur Auftragsverarbeitung mit den Unterauftragnehmern geschlossen