VEREINBARUNG
ZUR
AUFTRAGSVERARBEITUNG
zwischen

Kundenname (siehe Kopftext)
- nachfolgend „Auftraggeber" genannt -

und

KWS Kassen Waagen Software Vertriebs GmbH
Niedernberger Straße 11
63741 Aschaffenburg

- nachfolgend „Auftragnehmer" genannt -

Auftraggeber und Auftragnehmer werden nachfolgend gemeinsam als "Parteien" oder einzeln als "Partei" bezeichnet.

PRÄAMBEL

Diese Vereinbarung wird geschlossen, um den Anforderungen des Datenschutzrechts, insbesondere der Europäischen Datenschutzgrundverordnung (DS-GVO) Rechnung zu tragen. Die Parteien sind mit dem Auftrag /Wartungsauftrag von heute (nachfolgend „Leistungsvereinbarung") ein Auftragsverarbeitungsverhältnis gemäß Art. 28 DS-GVO) eingegangen. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung. Zudem vereinbaren die Vertragsparteien, dass bis zum Inkrafttreten der DS-GVO und der ggf. ergänzenden nationalen Gesetze in Deutschland, die analogen Regelungen des BDSG auf diese Vereinbarung Anwendung finden.

1. GEGENSTAND, DAUER

1.1 Gegenstand, Art und Zweck der Datenverarbeitung ergeben sich aus der Leistungsvereinbarung, auf die hier verwiesen wird.

1.2 Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Abrechnungs- und Finanzdaten mit Personenbezog

1.3 Der Kreis der durch den Umgang mit personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Ansprechpartner

1.4 Die Dauer dieser Vereinbarung (Laufzeit) entspricht der in der Leistungsvereinbarung vereinbarten. Diese Vereinbarung endet in jedem Fall automatisch mit Beendigung der Leistungsvereinbarung. Das Recht beider Parteien zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

1.5 Der Auftragnehmer ist Auftragsverarbeiter und der Auftraggeber ist Verantwortlicher im Sinne der DS-GVO.

2. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

2.1 Der Auftragnehmer wird die in der Anlage beschriebenen technischen und organisatorischen Maßnahmen in seinem Verantwortungsbereich durchführen. Diese Maßnahmen berücksichtigen den 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

2.2 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.

3. BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN

3.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach 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.

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

4. QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

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

4.1.1 Bestellung eines Datenschutzbeauftragten (DSB)

Der Auftragnehmer hat keinen DSB bestellt und ist dazu auch nicht aufgrund gesetzlicher Bestimmung verpflichtet. Sofern zukünftig eine gesetzliche Verpflichtung zur Bestellung eines DSB entsteht, wird der Auftragnehmer den Auftraggeber unverzüglich informieren und ihm die Kontaktdaten des bestellten DSB schriftlich mitteilen.

4.1.2 Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

4.1.3 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4.1.4 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.

4.1.5 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.

4.1.6 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.

4.1.7 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

5. KONTROLLRECHTE DES AUFTRAGGEBERS

5.1 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.

5.2 Der Auftragnehmer wird dafür Sorge tragen, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

5.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann alternativ erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz); die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO; oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO.

5.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

6. MITTEILUNG BEI VERSTÖßEN DES AUFTRAGNEHMERS

6.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

6.1.1 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

6.1.2 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

6.1.3 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

6.1.4 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

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

7. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

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

7.2 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.

8. LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

8.1 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.

8.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer auf Anfrage des Auftraggebers 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.

8.3 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.

9. RECHTE UND PFLICHTEN DES AUFTRAGGEBERS

Der Auftraggeber ist die verantwortliche Stelle für die Beurteilung der Zulässigkeit der Datenverarbeitung, -erhebung, -nutzung sowie für die Wahrung der Rechte der Betroffenen. Der Auftraggeber ist für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

10. RECHTE UND PFLICHTEN DES AUFTRAGNEHMERS

10.1 Ort der Verarbeitung und Nutzung von Daten

10.1.1 Die Verarbeitung und Nutzung der Daten durch den Auftragnehmer findet im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

10.1.2 Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DS-GVO erfüllt sind.

10.2 Unterauftragsverhältnisse, Art 28 Abs. 4 DS-GVO

Der Auftragnehmer kann zur Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbeziehen. Dabei hat der Auftragnehmer folgendes zu beachten:

10.2.1 Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen dieser Vereinbarung entsprechen.

10.2.2 Die Einschaltung von Unterauftragnehmern bedarf einer schriftlichen Beauftragung durch den Auftragnehmer.

10.2.3 Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

10.2.4 Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der

Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeber auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

10.2.5 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

11. SCHLUSSBESTIMMUNGEN

11.1 Änderungen oder Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform und sind von beiden Parteien zu unterzeichnen. Kündigungen bedürfen zu ihrer Wirksamkeit ebenfalls der Schriftform. Auch die Aufhebung der soeben vereinbarten Schriftform bedarf zu ihrer Wirksamkeit der Schriftform. Änderungen und Ergänzungen müssen als solche ausdrücklich gekennzeichnet sein.

11.2 Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen dadurch nicht berührt. Die Parteien werden die unwirksame Bestimmung unverzüglich durch eine solche wirksame ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

11.3 Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland.

11.4 Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist der Sitz des Auftragnehmers.

ANLAGE - TECHNISCH-ORGANISATORISCHE MAßNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

- Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

- Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.