Auftragsdaten-Verarbeitungs-Vertrag

Vereinbarung gemäß § 11 BDSG über die Auftragsdatenverarbeitung

zwischen der

Clarity & Success Software GmbH, Bokeler Str. 28, 33790 Halle/Westf.
sowie die damit verbundenen Unternehmungen
- nachstehend ***Auftragnehmer*** genannt –

und

KUNDEN

sowie seinen Filialen lt. Vertragsanlage
- nachstehend ***Auftraggeber*** genannt -

Vorwort:

Sehr geehrter Kunde/Auftraggeber,

im Laufe unserer künftigen Zusammenarbeit kann es vorkommen, dass wir für die Lösung eines Anliegens Ihre Clarity & Success-Datenbank benötigen, um beispielsweise Ursachenforschung zu vollziehen oder Korrekturen durchzuführen. Für solche Fälle schreibt das Datenschutzgesetz eine Vereinbarung vor, in der formal festgehalten wird, dass

a. Sie bereit sind, uns ggf. Ihre Daten zwecks Bearbeitung zur Verfügung zu stellen und
b. wir diese Daten absolut vertraulich behandeln und nach Beendigung des Auftrages auf unseren Systemen löschen, sofern sie nicht weiter benötigt werden

Deshalb ist es notwendig, die folgende Auftragsdatenvereinbarung zu bestätigen, damit Sie und wir dem Gesetz Genüge tun und Sie die Sicherheit haben, dass Ihre Daten bei Supportfällen geschützt sind.

Vielen Dank für Ihr Verständnis!

1. Geltungsbereich mit und ohne Vertragsanlage
Diese Vereinbarung gilt für die auf dem Deckblatt angegebene Verkaufsstelle bzw. Zentrale. Wird eine Vertragsanlage mit einer/mehreren Filialen beigefügt, wird sie zum Bestandteil dieser Vereinbarung mit den darin aufgeführten Filialen. Kommen künftig neue Filialen hinzu oder sollen welche ausgenommen werden, muss eine aktualisierte Vertragsanlage erstellt und dem Auftragnehmer gesendet werden, die die vorherige ersetzt, sofern nicht die Option „alle Filialen“ in der Anlage gewählt ist. Die Auftragsdatenvereinbarung selbst bleibt davon unberührt.

2. Gegenstand und Dauer des Auftrags
Gegenstand des Auftrags
Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
- ⇨ Datenbanken des eingesetzten Clarity & Success Warenwirtschafts- und Kassensystems und Daten jeglicher Art
- ⇨ Auftraggebern- und verkaufsspezifische Daten (Tagesabschlüsse, Lagerbewegung etc.)
- ⇨ Fernwartung auf Datenverarbeitungseinheiten des Auftraggebers ggf. mit Screenshots von dauerhaft benötigten Programmeinstellungen ohne jegliche personenbezogene Daten.

Die Dauer dieses Auftrags (Laufzeit) ist unbefristet bis auf Widerruf durch den Auftraggeber.

3. Konkretisierung des Auftragsinhalts
Umfang, Art und Zweck
der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten
Die Verarbeitung und Nutzung der Daten findet ausschließlich im **Gebiet** der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum beziehungsweise unter Anwendung des EU-U.S. Privacy Shield Framework statt. Jede sonstige Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.
Die **Erhebung** der Daten erfolgt durch Versenden durch den Auftraggeber an den Auftragnehmer oder durch Herunterladen über Fernwartung mit Kenntnis und Einverständnis des Auftraggebers. Die Verarbeitung dient ausschließlich zur Behebung von aufgetretenen Supportfällen oder zur Aktualisierung der Software oder der Datenbank sowie zur etwaigen Korrektur der Datenbank. Die Daten werden nicht anderweitig genutzt, nicht an Dritte weitergegeben und nach Abschluss der Arbeiten auf dem Clarity & Success-System gelöscht, sofern sie nicht mehr benötigt werden.

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende **Datenarten**: Personenstammdaten, Kundendaten, Verkaufsdaten, Artikeldaten, Lagerdaten, Lieferantendaten, Einkaufsdaten, Reparaturdaten, Mitarbeiterdaten.
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags **Betroffenen** umfasst: Kunden, Interessenten, Beschäftigte, Lieferanten, Handelsvertreter, Ansprechpartner.

4. Technisch-organisatorische Maßnahmen
Der Auftragnehmer hat für die technischen und organisatorischen Maßnahmen zum Schutz der Daten Sorge zu tragen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabe-Kontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots (vgl. Anlage zu dieser Vereinbarung), sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs/Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand, die - soweit sie sich nicht aus einer zugrundeliegenden Leistungsvereinbarung ergeben- nachstehend aufgeführt sind:

Die Maßnahmen im Einzelnen:
a. Zutrittskontrolle
Unbefugter Zutritt zu den Räumen wird verhindert durch:
- ⇨ Zutrittskontrollsystem (über Scannen und Erkennen des Fingerabdrucks)
- ⇨ Schlüssel / Schlüsselvergabe
- ⇨ Überwachungseinrichtung (Alarmanlage, Überwachungskameras, Objektschutz)

b. Zugangskontrolle
Das Eindringen Unbefugter in die Datenverarbeitungs-Systeme wird verhindert durch:

- ⇨ Schutz durch Server-Dienstleister
- ⇨ Schutz durch Firewall
- ⇨ Schutz durch Antivirus

c. Zugriffskontrolle

Unerlaubter Zugriff auf die Daten und das EDV-System wird verhindert durch:

- ⇨ Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- ⇨ Passwortschutz für alle Bereiche
- ⇨ Passwortschutz der Datenbank
- ⇨ Auswertungen
- ⇨ Kenntnisnahme

d. Weitergabekontrolle

Personenbezogene Daten werden bei Datentransport geschützt durch:

- ⇨ Tunnelverbindung (VPN = Virtual Private Network)
- ⇨ Protokollierung

e. Eingabekontrolle

Änderung und Löschung von Daten sind Nachvollziehbar durch:

- ⇨ Protokollierung

f. Verfügbarkeitskontrolle

Zur Datensicherung werden folgende Maßnahmen angewandt:

- ⇨ Backup-Verfahren
- ⇨ Spiegeln von Festplatten, z.B. RAID-Verfahren
- ⇨ Unterbrechungsfreie Stromversorgung (USV)
- ⇨ Getrennte Aufbewahrung
- ⇨ Virenschutz / Firewall
- ⇨ Notfallplan

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. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

5. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Kontrollen und sonstige Pflichten der Auftragnehmer

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- ⇨ Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt
- ⇨ Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebern zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- ⇨ Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- ⇨ Die unverzügliche Information des Auftraggebern über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG bei der Auftragnehmer ermittelt.
- ⇨ Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch die Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- ⇨ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

7. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer (die dann nicht als Dritte im Sinne dieser Vereinbarung gelten) einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- ⇨ Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer entsprechen.
- ⇨ Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer 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.

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, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8. Kontrollrechte des Auftraggebern

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit der dem Auftragnehmer 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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

9. Mitteilung bei Verstößen der Auftragnehmer

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat die Auftragnehmer ihn hierbei zu unterstützen.

10. Weisungsbefugnis des Auftraggebern

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam

abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggebern bestätigt oder geändert wird.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Vereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

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.

12. Erfordernis der Anpassung dieses Vertrags aufgrund der Rechtsentwicklung

Erwägungsgrund Nr. 171 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung) enthält die Vorgabe, dass die Richtlinie 95/46/EG durch diese Verordnung aufgehoben werden soll. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden.

Auftraggeber und Auftragnehmer sind sich daher - sofern der vorliegende Auftrag über die personenbezogene Datenverarbeitung nach dem Zeitpunkt der Anwendung der Datenschutz-Grundverordnung fortgeführt werden soll - darüber einig, dass es zum Zweck der Einhaltung der in Artikel 28 der Datenschutz-Grundverordnung enthaltenen Vorgaben zwingend erforderlich werden wird, künftig einen diesen Vorgaben entsprechenden Vertrag über die Auftragsverarbeitung zu schließen, der an die Stelle des vorliegenden tritt.

Ort, Datum

Unterschrift Clarity & Success Software GmbH
Dipl.-Ing. Florian Henkel
Managing Director
(Auftragnehmer)

Ort, Datum

Unterschrift Kunde
(Auftraggeber)

Anlage zu dieser Vereinbarung folgt auf der nächsten Seite.

Anlage zur Auftragsdatenvereinbarung

Datum:

Die Auftragsdatenvereinbarung soll neben der Zentrale auch für sämtliche bestehende und künftige Filialen in folgenden Ländern gelten:

Nur in folgenden Filialen:

Kd.-Nr. (Auftraggeber-Nr.)	Filial-Name	Land