Allgemeinen Bedingungen zur Auftragsverarbeitung des IT-Service-Unternehmens Daniel Stange „The Computer Factory“

1. ALLGEMEINES

Gegenstand der Vereinbarung ist die Vereinbarung der Rechte und Pflichten des Kunden (nachfolgend auch „Auftraggeber“) und des IT-Service-Unternehmens Daniel Stange „The Computer Factory“ (nachfolgend auch „Auftragnehmer“ oder „TCF“ genannt) sofern im Rahmen der Leistungserbringung eine Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten für den Kunden durch TCF erfolgt.

2. GEGENSTAND UND DAUER DES AUFTRAGES

TCF verarbeitet insbesondere im Rahmen des IT-Service personenbezogene Daten im Auftrag des Kunden. Der Umfang der Tätigkeit ergibt sich aus dem TCF erteilten Auftrag. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

3. KONKRETISIERUNG DES AUFTRAGSINHALTS

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

TCF erhebt, verarbeitet und nutzt personenbezogene Daten, welche im Rahmen von Vertriebs- insbesondere aber auch Serviceprozessen entstehen oder an TCF übergeben werden. Die Verarbeitung und Nutzung der Daten findet im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 – 50 EU-DSGVO erfüllt sind. Zu Zwecken der Auftragsrealisierung, insbesondere im Zusammenhang mit der Generierung von Softwarelizenzschlüsseln, können Daten in Drittländer übermittelt werden, wenn und soweit die Übermittlung zur Erfüllung eines Vertrags mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist.

3.2 Art der Daten/Kreis der Betroffenen

Die Art und Menge der genutzten personenbezogenen Daten und betroffenen Personengruppen hängt vom Einsatz/ Nutzung des Leistungsgegenstandes des Hauptvertrages ab. Folgende Arten von Daten können betroffen sein: Vorname, Nachname, E-Mail-Adresse, Telefonnummern, PLZ, Ort, Straße, Hausnummer, angebotene oder erworbene/genutzte Waren sowie Dienstleistungen. In der Regel stammen diese Daten aus Datenbanken von ERP-Systemen, Daten aus Microsoft-Anwendungen, insbesondere Microsoft-Exchange-Daten oder vergleichbare Lösungen. Der Kreis der Betroffen sind vorrangig die Nutzer dieser Systeme.

4. TECHNISCH-ORGANISATORISCHE MAßNAHMEN (TOM)

Der Auftragnehmer hat technische und organisatorische Maßnahmen vor Beginn der Verarbeitung dokumentiert. Die Dokumentation (Datenschutzkonzept) erfolgt im Rahmen der Qualitätsfestlegungen, welche nach DIN EN ISO 9001 strukturiert, jedoch nicht zertifiziert sind. Der Auftragnehmer hat auf Anforderung die Angaben nach Artikel 30 Abs. 2 EU-DSGVO dem Auftraggeber zur Verfügung zu stellen. Ohne gesonderte Prüfung wird von einer Akzeptanz der TOM durch den Auftraggeber ausgegangen. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung etc. Diese 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.

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 DES AUFTRAGNEHMERS

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Artikel 28 EU-DSGVO folgende Pflichten:

- Die Wahrung des Datengeheimnisses entsprechend Artikel 28 Abs. 3 b EU-DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, werden auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen (TOM) entsprechend. Artikel 32 EU-DSGVO.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Artikel 57 und 58 EU-DSGVO. Dies gilt auch, soweit eine zuständige Behörde nach. Artikel 57 und 58 EU-DSGVO beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den 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.

7. UNTERAUFTRAGSVERHÄLTNISSE

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit Zustimmung des Auftraggebers gestattet. Ohne Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Ziffer 6 erläuterten Pflicht zur Auftragskontrolle Vertrags-Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen. Subunternehmer sind für den Auftragnehmer mit lt. QM-Richtlinien dokumentierten Auftragsinhalten in dem dort genannten Umfang tätig. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. TCF ist berechtigt, mit einer angemessenen Ankündigungsfrist diese Subunternehmer gegen andere Subunternehmer auszutauschen. Dabei werden die Interessen des Kunden angemessen berücksichtigt. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung Artikel 28 Abs. 3 d i. V. m. Artikel 28 Abs. 2 und 4 EU-DSGVO 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. Ebenso sind Hersteller von Softwaremodulen (z. B. Plug-ins oder Add-ons) bzw. Integrationen, die lediglich eine von TCF zur

Verfügung gestellte Schnittstellen nutzen, keine Subunternehmer im Sinne dieser Vereinbarung.

8. KONTROLLRECHTE DES AUFTRAGGEBERS

Der Auftraggeber hat das Recht, die in Artikel 32 EU-DSGVO vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig (mindestens 7 Werktage vorher) 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. Der Auftraggeber lässt die Kontrolle nur durch eine Person durchführen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse und Sicherheitsmaßnahmen verpflichtet ist. Der Auftragnehmer behält sich vor, etwaig entstehende interne oder externe Kosten für diese Kontrollen in den Geschäftsräumen des Auftragnehmers dem Auftraggeber in Rechnung zu stellen. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Artikel 28 Abs. 3 h) EU-DSGVO 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 Art. 32 EU-DSGVO 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 DES AUFTRAGNEHMERS

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 Art. 33 und 34 EU-DSGVO) 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 Art. 33 und 34 EU-DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

10. WEISUNGSBEFUGNIS DES AUFTRAGGEBERS

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (Art. 28 Abs. 3 a) EU-DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass 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, per E-Mail (in Textform) oder per Fax bestätigen. 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 (Art. 28 Abs. 3, letzter Absatz) zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt (aber nicht verpflichtet), die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber schriftlich oder per Telefax 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 Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, vorbehaltlich anderer vertraglicher Absprachen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Protokolle der Löschung werden auf Anforderung des Auftraggebers erstellt. 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. WAHRUNG VON GESCHÄFTSGEHEIMNISSEN

Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekannt werdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden, vorbehaltlich anderer vertraglicher Absprachen. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig. Die vorgenannte Verpflichtung findet insoweit keine Anwendung, als die Partei darlegen kann, dass Informationen öffentlich zugänglich und zum Zeitpunkt der Offenlegung verfügbar oder danach der Öffentlichkeit zugänglich geworden sind, und zwar ohne Verletzungshandlung oder -unterlassung durch diese Partei oder eines ihrer Vertreter oder Angestellten, oder vor dem Erhalt von der anderen Partei im Besitz der Partei oder ihr bekannt waren, oder der Partei durch eine andere Person ohne Einschränkung rechtmäßig offen gelegt wurden, oder von der Partei ohne Zugang zur Information der anderen Partei unabhängig entwickelt wurden, oder nach gesetzlichen oder verwaltungsrechtlichen Vorschriften offen gelegt werden müssen, wenn der anderen Partei dieses Erfordernis unverzüglich bekannt gegeben wird und der Umfang solcher Offenlegung soweit wie möglich eingeschränkt wird, oder aufgrund einer gerichtlichen Entscheidung offen gelegt werden müssen, wenn der anderen Partei von dieser Entscheidung unverzüglich Nachricht gegeben wurde und wenn nicht die Möglichkeit besteht, diese Entscheidung anzufechten.

13. KONTAKTPERSONEN

Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der jeweils anderen Partei gegeben werden, sind sie an die Geschäftsführung der TCF als Weisungsberechtigten oder -empfänger zu richten und an die im Auftrag als Bearbeiter benannte Person zu richten. Jede Partei kann einseitig ihre Kontaktpersonen durch schriftliche Erklärung gegenüber der anderen Partei ändern.

Datenschutzkonzept:

Technische und organisatorische Maßnahmen (früher Anlage zu § 9 BDSG) der TCF zur Umsetzung der EU-DSGVO und zur Einhaltung der internen Datenschutzstandards/Qualitätsrichtlinien

1. Zutrittskontrolle

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

□ Alarmanlage

□ Manuelles Schließsystem (Sicherheitsschlösser) mit Sicherungskarte

□ Sicherheitscheck beim Verlassen des Gebäudes

□ Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

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

□ Passwortvergabe lt. definierter Kennwortrichtlinie des Servers

□ Authentifikation mit Benutzername/Passwort

□ Einsatz von VPN-Technologie

□ Einsatz von Fernwartungssoftware welche von Herstellern stammen, die konform zu den Service Organization Controls 2 (SOC2)-Richtlinien agieren

□ Sorgfältige Auswahl von Reinigungspersonal

□ Einsatz einer Hardware- und Software-Firewall

3. 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.

□ Erstellen eines Berechtigungskonzepts

□ Anzahl der Administratoren auf das „Notwendigste“ reduziert

□ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

□ Löschung von Datenträgern vor Wiederverwendung

□ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

□ Verwaltung der Rechte durch Systemadministrator

□ Verwaltung externer Datenträgern inkl. Cloud

□ Sichere Aufbewahrung von Datenträgern im Serverschrank / Tresor verschlossen

□ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

□ Protokollierung der Vernichtung (auf Kundenwunsch)

4. 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 dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

□ Einrichtungen von Fernzugriffen / VPN

□ Dokumentation der Empfänger von Daten

□ Beim Physischen Transport: Serviceschein / Arbeitsauftrag

5. Eingabe Kontrolle

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

□ Protokollierung der Eingabe, Änderung und Löschung von Daten im ERP- System

□ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen);
ausschließlich im ERP- System

□ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

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

□ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

7. Verfügbarkeitskontrolle

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

Unterbrechungsfreie Stromversorgung (USV)

Überwachung von Temperatur im Serverschrank

Schutzsteckdosenleisten in Serverschrank

Feuer- und Rauchmeldeanlagen

Feuerlöschgeräte in/vor Serverräumen

Erstellen eines Backup- & Recoverykonzepts

Testen von Datenwiederherstellung

Aufbewahrung von Datensicherung an einem sicheren,
ausgelagerten Ort

8. Trennungsgebot

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

Logische Mandantentrennung (softwareseitig)

Erstellung eines Berechtigungskonzeptes

getrennte Datenbanken

Festlegung von Datenbankrechten

Trennung von Produktiv- und Testsystem

Dessau-Roßlau, Mai 2018

Daniel Stange

Digital unterschrieben
von Daniel Stange
Datum: 2018.05.24
17:40:33 +02'00'

Daniel Stange
Inhaber
The Computer Factory