

Auftragsdatenverarbeitung

Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG

zwischen

dem Kunden

- nachstehend Auftraggeber oder Kunde genannt -

und

TecArt GmbH

- nachstehend Auftragnehmer genannt -

- nachstehend einzeln oder gemeinsam auch Parteien genannt -

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (nachfolgend auch „ADV“) ergänzt den zwischen den Parteien geschlossenen Vertrag inkl. sämtlicher bestehender oder künftiger Zusatzvereinbarungen oder sonstiger ergänzender Vereinbarungen (nachstehend „Hauptvertrag“ genannt). Soweit der Auftragnehmer im Zusammenhang mit der Erfüllung seiner Leistungsverpflichtung aus dem Hauptvertrag für den Auftraggeber personenbezogene Daten (nachfolgend auch „Daten“) erhebt, verarbeitet oder nutzt bzw. der Zugriff auf solche Daten nicht ausgeschlossen werden kann, regeln sich die Datenschutzanforderungen an den Umgang mit diesen Daten nach dieser ADV.

Soweit sich die Konkretisierung einzelner Teile der ADV erst aus Einzelvereinbarungen, Aufträgen, Leistungsscheinen, Pflichtenheften etc. (Einzelauftrag) ergibt, sind die entsprechenden Datenschutzanforderungen in gesonderten Einzelvereinbarungen zur Verarbeitung personenbezogener Daten im Auftrag zum jeweiligen Einzelauftrag (Einzel-ADV) zu konkretisieren. In diesem Fall darf der Umgang mit personenbezogenen Daten des Auftraggebers erst nach Abschluss einer vollständigen Einzel-ADV hierfür erfolgen.

§ 2 Leistungen des Auftragnehmers

(1) Die Möglichkeit, dass der Auftragnehmer Zugriff auf folgende personenbezogene Daten hat, kann nicht ausgeschlossen werden:

- Anwendungsdaten der Kunden
- Anwendungsdatenbank des Kunden (z.B. MySQL)
- Über die Anwendung im Dateisystem abgelegte Dokumente
- Über die Anwendung empfangene E-Mails

Eine genauere Klassifizierung der Daten ist nicht möglich, da es sich bei der Anwendung um ein frei konfigurierbares System handelt und die Art der von den Kunden erfassten Daten innerhalb der Anwendung vor Inbetriebnahme nicht ersichtlich ist. Hierbei handelt es sich ausschließlich um die vom Kunden selbst in seiner Anwendung erfassten Daten.

(2) Der Auftragnehmer erbringt für den Auftraggeber Prüf- bzw. Wartungstätigkeiten, die sich im Einzelnen aus dem Hauptvertrag ergeben.

§ 3 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Wartung zu erteilen.

(2) Der Auftraggeber kann jederzeit und unverzüglich die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarung durch den Auftragnehmer, auch in dessen Betriebsstätten, kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme beim Auftragnehmer. Er darf das Ergebnis der Kontrollen dokumentieren. Der Auftraggeber kann die Kontrollen selbst durchführen oder durch einen beauftragten Dritten durchführen lassen. Der Auftragnehmer ist entsprechend zur Auskunft und Mitwirkung verpflichtet. Der Auftragnehmer unterstützt den Auftraggeber insbesondere bei Datenschutzkontrollen durch die Aufsichtsbehörde, soweit es sich um die Datenverarbeitung im Rahmen dieser Vereinbarung handelt, und setzt Anforderungen der Aufsichtsbehörde in Abstimmung mit dem Auftraggeber unverzüglich um.

(3) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge und Weisungen schriftlich, per Telefax oder per E-Mail.

§ 4 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer erbringt für den Auftraggeber bezogen auf die Daten im Hauptvertrag vereinbarten Leistungen. Ist dabei der Zugriff auf Daten wegen der Art der vereinbarten Prüf- bzw. Wartungstätigkeit, Reparaturen oder wegen des Austauschs von Komponenten unvermeidbar, so verpflichtet sich der Auftragnehmer, den Datenzugriff auf das unverzichtbare Mindestmaß zu beschränken. Dabei ist ein Zugriff auf Daten des Auftraggebers zu vermeiden. Ist dies nicht möglich, ist dies mit dem Auftraggeber abzustimmen. Soweit ein Zugriff auf Daten des Auftraggebers erforderlich ist, verwendet der Auftragnehmer die Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, ausschließlich für Zwecke der Wartung im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(2) Der Auftragnehmer ist verpflichtet, alle im Rahmen der Leistungserbringung erlangten Kenntnisse durch gegebenenfalls erforderlichen Zugriff auf Daten des Auftraggebers, von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zu bringen. Der Auftragnehmer ist insbesondere nicht berechtigt, Daten des Auftraggebers an Dritte weiterzugeben.

(3) Wurden Daten des Auftraggebers im Zuge der Wartung kopiert oder ausgedruckt, so sind diese nach Abschluss der konkreten Maßnahme unverzüglich zu löschen oder zu vernichten. Datenträger, die der Auftraggeber für die Arbeiten zur

Verfügung gestellt hat, sind dem Auftraggeber unmittelbar nach Abschluss der Arbeiten wieder auszuhändigen.

(4) Die Leistungserbringung der unter § 2 bzw. im Hauptvertrag vereinbarten Leistungen darf grundsätzlich nur in Deutschland erfolgen. Eine Leistungserbringung in Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, ist nur nach schriftlicher Bestätigung durch den Auftraggeber für den vereinbarten Einzelfall zulässig. Eine Leistungserbringung in anderen Ländern (sog. Drittstaaten) ist unzulässig.

(5) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellten Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

(6) Der Auftragnehmer sichert zu, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt zu haben, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird. Der Datenschutzbeauftragte hat die Aufgaben gem. § 4g Bundesdatenschutzgesetz (BDSG) wahrzunehmen, er hat insbesondere auf die Einhaltung der gesetzlichen und der vereinbarten Regelungen zum Datenschutz hinzuwirken. Zu den Kontaktdaten des betrieblichen Datenschutzbeauftragten des Auftragnehmers s. unten § 6 Absatz 2.

(7) Ist der Auftraggeber gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Daten zu geben, so wird der Auftragnehmer den Auftraggeber darin unterstützen, diese Auskünfte zu erteilen. Im Fall von Datenschutzverletzungen, die mit der Datenerhebung, -verarbeitung bzw. -nutzung durch den Auftragnehmer im Zusammenhang stehen, unterstützt der Auftragnehmer den Auftraggeber auf Aufforderung bei der Benachrichtigung Betroffener und der Aufsichtsbehörde. Der Auftragnehmer informiert den Auftraggeber außerdem unverzüglich über jegliche Kommunikation der Aufsichtsbehörden (z.B. Anfragen, Mitteilung von Maßnahmen oder Auflagen) gegenüber dem Auftragnehmer im Zusammenhang mit der Datenerhebung, -verarbeitung oder -nutzung unter dieser Vereinbarung. (8) Soweit nicht ausdrücklich anders vereinbart, ist der Auftragnehmer in allen anderen Fällen nicht berechtigt ohne vorherige Zustimmung des Auftraggebers Auskünfte über zu den Daten zu machen. Auskünfte an Dritte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(9) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

§ 5 Datengeheimnis, Fernmeldegeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der Datenverarbeitung das Datengeheimnis gemäß derzeit § 5 BDSG und das Fernmeldegeheimnis gemäß derzeit § 88 Telekommunikationsgesetz (TKG) zu wahren.

Er verpflichtet sich im Übrigen, die jeweils geltenden gesetzlichen Datenschutzbestimmungen zu beachten, derzeit insbesondere die des BDSG, des TKG und des Telemediengesetzes (TMG).

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind, und sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter nachweislich zuvor mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und insbesondere auf das Datengeheimnis gemäß § 5 BDSG und das Fernmeldegeheimnis nach § 88 TKG verpflichtet. Er

überwacht im Übrigen die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Die Verpflichtung zum Datengeheimnis und Fernmeldegeheimnis gilt auch nach Beendigung dieser Vereinbarung fort.

§ 6 Ansprechpartner der Parteien

(1) Fachlicher Ansprechpartner des Auftragnehmers ist:

Ansprechpartner: Ronny Richter

Funktion: Leiter Back Office und Support

E-Mail: support@tecart.de

(2) Datenschutzbeauftragter des Auftragnehmers ist:

Datenschutz-

beauftragter: Ronny Kümmel

E-Mail: datenschutz@tecart.de

(3) Der Ansprechpartner des Auftraggebers ist im Hauptvertrag benannt.

§ 7 Technische und organisatorische Sicherheitsmaßnahmen

(1) Der Umgang mit den Daten des Auftraggebers, die er dem Auftragnehmer bereitstellt, auf die er den Zugriff ermöglicht, die Ergebnis des Auftrags sind oder die auf sonstige Weise bei der Auftragsabwicklung durch den Auftragnehmer anfallen oder durch ihn zur Kenntnis genommen werden können, erfolgt ausschließlich unter Beachtung der erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage hierzu. Diese derzeit erforderlichen Maßnahmen sind in Anlage 1 beschrieben.

(2) Soweit die mit dem Auftraggeber vereinbarten Sicherheitsmaßnahmen aus Sicht des Auftragnehmers durch technischen Fortschritt unwirtschaftlich geworden sind oder keinen angemessenen, zeitgemäßen Schutz mehr bieten, benachrichtigt der Auftragnehmer den Auftraggeber. Der Auftraggeber hat das Recht die Sicherheitsmaßnahmen durch wirksamere Verfahren anpassen zu lassen. Die Maßnahmen werden erst nach entsprechender Weisung des Auftraggebers ausgeführt. Der Auftraggeber ersetzt dem Auftragnehmer den durch die Anpassung der Schutzmaßnahmen nach § 9 BDSG an den technischen Fortschritt entstehenden Mehraufwand.

(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren. Vor Durchführung der Prüfungs- und Wartungsarbeiten werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherungsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(4) Alle Prüfungs- und Wartungsarbeiten, auch solche im Weg des Fernzugriffs, werden dokumentiert und protokolliert.

(5) Der Auftragnehmer wird von den, ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten unerlässlich notwendig ist.

(6) Der Auftragnehmer wird Daten auf Speichermedien, die er aufgrund von Prüfungs- oder Wartungsarbeiten im Rahmen eines Austauschs, einer Vertragsaufhebung oder zur Vernichtung erhält, dauerhaft löschen. Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen sind in Anlage 1 beschrieben. Das zur Datenlöschung angewandte Verfahren wird einem Qualitätsmanagementsystem unterworfen, die Datenlöschung wird dokumentiert.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z.B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten des

Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Zustimmung des Auftraggebers einholen. Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Zustimmung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Zustimmung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks, CDs, DVDs oder ähnliche Geräte) kopiert werden.

§ 8 Subunternehmer

(1) Der Auftragnehmer stellt sicher, dass Subunternehmer gegenüber dem Auftragnehmer in entsprechender Weise verpflichtet sind, wie der Auftragnehmer gegenüber dem Auftraggeber nach dieser Vereinbarung verpflichtet ist. Der Auftragnehmer hat die Einhaltung dieser Pflichten des Subunternehmers, insbesondere die Einhaltung der dort vereinbarten technischen und organisatorischen Maßnahmen, vor dem erstmaligen Beginn der Prüf- bzw. Wartungstätig und sodann regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren.

(2) Der Auftragnehmer stellt ferner sicher und sichert vertraglich ab, dass der Auftraggeber gegenüber dem Subunternehmer die gleichen Kontrollrechte hat wie der Auftraggeber sie gegenüber dem Auftragnehmer selbst hat. Diese vertragliche Absicherung ist so zu gestalten, dass sie den Auftraggeber - unbeschadet der Verantwortlichkeit des Auftragnehmers für den Subunternehmer - unmittelbar gegenüber dem Subunternehmer berechtigt. Auf Anforderung ist der Auftragnehmer verpflichtet, dem Auftraggeber Auskunft über den für die Kontrollrechte wesentlichen Vertragsinhalt und über die Umsetzung der datenschutzrelevanten Verpflichtungen durch den Subunternehmer zu geben.

§ 9 Vertragsdauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages. Sollten Leistungen auch noch nach der Laufzeit des Hauptvertrags erbracht werden, gelten die Regelungen dieser Vereinbarung auch für diese weitere Leistungserbringung für die gesamte Dauer der tatsächlichen Kooperation fort.

§ 10 Nutzungsrechte

Dem Auftragnehmer werden bzgl. der Daten keine Nutzungsrechte gewährt, die über die nach dieser Vereinbarung geregelte Verarbeitung hinausgehen.

§ 11 Sonstiges

Im Übrigen gelten ergänzend die Schlussbestimmungen aus den jeweiligen Allgemeinen Geschäftsbedingungen der TecArt GmbH in der jeweils geltenden Fassung (Ziffer 21., Stand 1. Juli 2012).

Anlage 1

So sicher sind Ihre Daten bei der TecArt GmbH!

Das Thema Cloud Computing überschwemmt den IT-Markt in den letzten Jahren wie kein anderes Thema. Zwar war das Modell der Softwarenutzung über einen Webbrowser und das Hosting von Daten in firmenexternen Rechenzentren bereits unter den Namen "ASP" oder "SaaS" bekannt aber erst der Begriff "Cloud" etablierte diese Variante des Softwarebezugs gegenüber dem traditionellen Software-Lizenzmodell zum Kauf vollends. Mit steigendem Interesse an einer Cloud-Lösung wuchsen bei den Interessenten auch immer mehr Fragen zur Datensicherheit und zum Datenschutz, die zum fundamentalen Kriterium wurden. Die Flut an erscheinenden Artikeln mit diesem Themenbezug zeugen von diesem Trend.

Als Hersteller einer Cloud-Lösung widmen wir uns natürlich intensiv diesem Thema und möchten Ihnen verdeutlichen, welche Sicherheitsmaßnahmen wir vornehmen, um Ihre Daten jederzeit zu schützen. Eine Zusammenfassung der ausschlaggebenden Sicherheitsvorteile, die Sie bei Nutzung des TecArt-CRM erhalten unter Einbezug des rechtlichen Datenschutzes, haben wir für Sie im weiteren Text aufgezeigt.

Ausschlaggebende Sicherheitsvorteile

1. Ihre Daten liegen in deutschen Rechenzentren

Die TecArt GmbH ist deutscher Softwarehersteller und hat somit rechtlich seinen Firmensitz in Deutschland. Damit unterliegt TecArt automatisch den Datenschutzbestimmungen des europäischen Datenschutzrechtes, d.h. für Sie, Ihre Daten liegen in deutschen (europäischen) Rechenzentren und dürfen diese auch nicht verlassen. Anders verhält sich das bei Anbietern, die zwar auch ihre Daten in europäischen Rechenzentren hosten ABER ihren Firmensitz z.B. in den USA haben. Für diese Firmen gilt das dortige Gesetz. Damit dürfen us-amerikanische Behörden und Regierungsstellen ohne Ihre vorherige Zustimmung auf die gespeicherten Daten auch in europäischen Rechenzentren zugreifen. Mit der TecArt GmbH als deutscher Hersteller können Sie dieses Risiko vermeiden. Wenn Sie darüber mehr erfahren möchten, lesen Sie weitere Artikel unter www.heise.de

2. Anwendung der Auftragsdatenverarbeitung nach Paragraph 11 des BDSG

Für Cloud-Anwendungen gilt das Auftragsdatenverarbeitungsgesetz laut Paragraph 11 BDSG in dem die Verarbeitung und Speicherung der Daten geregelt ist. Mit Ihrem Auftrag erteilen Sie uns direkt die Genehmigung zur Speicherung der personenbezogenen Daten. Eine Verarbeitung Ihrer Daten nehmen wir selbst nicht vor. Wir liefern Ihnen lediglich das Werkzeug mit dem Sie Ihre Daten selbst verarbeiten können. Wir garantieren Ihnen so das Eigentum an Ihren Kundendaten und die alleinigen Rechte, damit sind ausschließlich Sie für den Datenschutz Ihrer Daten weiterhin verantwortlich. Wir besitzen mit Ihrem Auftrag nicht das Recht zur "Weitergabe an Dritte".

3. Erfüllen Sie mit uns die "8 Gebote des Datenschutzes" für Cloud Computing

Laut Gesetz müssen Sie als Auftraggeber die Voraussetzungen für die Auftragsdatenverarbeitung prüfen. Das heißt, Sie müssen uns als Vertragspartner unter besonderer Berücksichtigung der Eignung der von uns getroffenen technischen und organisatorischen Maßnahmen per Paragraph 9 BDSG sorgfältig prüfen. Dazu regelt die Anlage des genannten Paragraphen die Kriterien. Wir helfen Ihnen gern dabei und zeigen Ihnen mit welchen professionellen Maßnahmen wir Sie unterstützen den Paragraph 9 einzuhalten:

(1) Unbefugten ist der Zutritt zu unseren zertifizierten Datenverarbeitungsanlagen nicht gewährt. Nur über eine schriftliche Zutrittsgenehmigung, welche ausschließlich durch uns bei dem entsprechenden Rechenzentrum im Vorfeld eingereicht wird, kann ein Zutritt nach Prüfung und Erlaubnis des Rechenzentrums stattfinden. (Zutrittskontrolle)

(2) Durch von uns bereitgestellte Sicherheitsmechanismen, wie ein persönliches Login und Passwort, eine persönliche Sicherheitsabfrage und dem IT-Zugriffsschutz, ermöglichen wir Ihnen die Nutzung des Systems durch Unbefugte zu verhindern. (Zugangskontrolle)

(3) Unsere umfassende administrative Rechtevergabe für Gruppen und Benutzer reicht bis hin zum personenbezogenen Lese-, Bearbeitungs- und Schreibschutz von Modulen, Kontakten, Projekten oder auch Ordnern und Dokumenten. Somit können Sie detailliert einstellen, dass "Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können". (Zugriffskontrolle)

(4) Durch unsere SSL-Verschlüsselung besteht eine gesicherte und verschlüsselte Datenübertragung zwischen Server und Client. Somit können die Daten während ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. (Weitergabekontrolle)

(5) Durch unseren Überschreibschutz und dem rechtsspezifischen Schutz vor unbefugtem Löschen von Dokumenten und Objekten gewährleistet unser System, "dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind". (Eingabekontrolle)

(6) Mit Ihrem Auftrag haben Sie uns nur die Speicherung Ihrer Daten und die Auslieferung unseres Systems als Werkzeug genehmigt. Eine Verarbeitung Ihrer Daten nehmen wir nicht vor, somit verlangen wir niemals die Zusendung von Kundendaten oder Ihren Passwörtern. Sollten Sie uns diese doch aus Versehen mitteilen, sind all unsere Mitarbeiter geschult jederzeit vertraulich mit diesen Informationen umzugehen. (Auftragskontrolle)

(7) Ihre Daten sind gegen zufällige Zerstörung oder Verlust geschützt durch einen integrierten Papierkorb für jeden Nutzer, eine systeminterne Backup-Funktion von bis zu 30 Tagen sowie separate Backup-Server zur täglichen Datensicherung mit 7-tägiger Vorhaltdauer. (Verfügbarkeitskontrolle)

(8) Unser System bietet Ihnen die Möglichkeit, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. (Trennungskontrolle)