Zusatzvereinbarung zur Auftragsdatenverarbeitung

zum Vertrag / zu den Verträgen

unter der

Kundennummer _____

Auftragsnummer _____

zwischen

Name: _____

Straße: _____

PLZ / Ort :_____

nachfolgend

- **Auftraggeber** / **Kunde** -

und

STRATO AG
Pascalstraße 10
10587 Berlin

nachfolgend

- **Auftragnehmer** -

Präambel

Diese Zusatzvereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag (Angebot / Leistungsbeschreibung, AGB) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Definitionen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftragnehmer erbringt Hostingleistungen für Webhosting-Pakete, Online-Festplatten, Internet-Shops, dedizierte und virtuelle Server. Die Leistungen umfassen je nach Paket die Bereitstellung von Speicherplatz, elektronischen Postfächern, Datenbanken und Skripten. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG). Die Art der personenbezogenen Daten und der Verarbeitungszweck werden in **Anlage 1** näher beschrieben.

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe seiner Daten verlangen, soweit der Auftraggeber dies mit seinen Zugriffen nicht selbst durchführen kann.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf die Daten des Auftraggebers (Anlage 1) nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten / Aufwendungen vom Auftraggeber zu tragen.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Eine Auflistung dieser technischen und organisatorischen Maßnahmen wird als **Anlage 2** beigefügt.

(3) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG (Verfahrensverzeichnis) notwendigen Angaben zur Verfügung.

(4) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten, soweit die Daten des Auftraggebers betroffen sind.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

(4) Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.

(5) Die Daten werden nach dem Ende des jeweiligen Vertrages gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen Daten anzufertigen und die Daten vor Vertrags-

ende umzuziehen. Der Auftraggeber hat selbst Zugriff auf seine Daten. Eine Pflicht des Auftragnehmers zur Herausgabe besteht daher nicht.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Voraussetzung ist, dass der Auftraggeber den Auftragnehmer hierzu schriftlich aufgefordert und ihm die durch diese Unterstützung entstandenen Kosten erstattet.

§ 6 Kontrollrechte

(1) Der Auftraggeber kann sich auf seine Kosten vor der Aufnahme der Datenverarbeitung und sodann jederzeit von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. In der Regel erfolgt diese Überzeugung durch die Einholung von Selbstauskünften des Auftragnehmers oder die Vorlage eines Zertifikates des Auftragnehmers. Der Auftragnehmer lässt sich zur Zeit regelmäßig vom TÜV Süd nach ISO 27001 auf Datensicherheit hin überprüfen. Der Auftraggeber kann die Vorlage dieses Zertifikates verlangen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

(3) Sollte dem Auftraggeber die Selbstauskunft oder das Zertifikat nicht ausreichen - etwa wegen der Sensitivität der verarbeiteten Daten oder des Gefährdungspotentials -, kann der Auftraggeber sich durch einen anerkannten Sachverständigen für IT-Datenschutz (TÜV-Prüfer oder vergleichbar) vor Ort von den technischen und organisatorischen Maßnahmen überzeugen. Die Kontrolle vor Ort kann nur nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs erfolgen. Der Auftragnehmer kann eine Erstattung seines Aufwandes (Personalkosten u. a.) verlangen.

(4) Der Auftraggeber kann die Ergebnisse der Prüfung dokumentieren und die Ergebnisse / Dokumentation für den Nachweis der Erfüllung seiner Sorgfaltspflichten gemäß § 11 BDSG verwenden, soweit Geheimhaltungsinteressen oder Sicherheitsinteressen des Auftragnehmers dem nicht entgegenstehen. Der Auftraggeber ist sich bewusst, dass jede weitere Verwendung Geheimhaltungsinteressen und Sicherheitsinteressen des Auftragnehmers gefährden und diesem Schaden zufügen kann. Die Geheimhaltungspflicht besteht auch im Interesse aller anderen Kunden, weil die Veröffentlichung der Sicherheitsmaßnahmen die Sicherheit der Rechenzentren gefährdet. Keinesfalls dürfen Ergebnisse Dritten mitgeteilt oder veröffentlicht werden.

§ 7 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungspflichten verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. dritte Unternehmen mit Leistungen unterbeauftragt.

(2) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages.

§ 8 Informationspflichten, Annahmeerklärung, Schriftformklausel, AGB

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

(2) Der Auftraggeber verzichtet auf die Erklärung der Annahme durch den Auftragnehmer (§ 151 Satz 1 BGB).

(3) Änderungen und Ergänzungen dieser Zusatzvereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Im übrigen gelten die Allgemeinen Geschäftsbedingungen des Auftragnehmers.

_____, den _____

_____
Auftraggeber

Anlagen

Anlage 1 - Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung

Anlage 2 - Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen gemäß §§ 11, 9 BDSG und Anlage

Anlage 1 - Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung

1. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung

Datenverarbeitungszweck ist die Erbringung der technischen Leistungen für die Bereitstellung der Dienstleistungen der STRATO AG, wie sie in den Angeboten / Leistungsbeschreibungen und den AGB der STRATO AG beschrieben werden.

2. Art der Daten*

Daten, die der Auftraggeber oder von ihm autorisierte Nutzer in den bereit gestellten Paketen (Webhosting-Pakete, Online-Speicher, E-Shops, dedizierte und virtuelle Server) speichern (Inhalt der Webseiten, des Online-Speichers, der Datenbanken etc.)

☐ Adressdaten	☐ Abrechnungsdaten	☐ E-Mails
☐ Angebotsdaten	☐ Finanzdaten	☐ Video- / Bilddateien
☐ Bankverbindungsdaten	☐ Mitarbeiterdaten	☐ Nutzungsdaten
☐ Bestelldaten	☐ Leistungsdaten	☐ Interessen / Profile
☐ Kontaktdaten	☐ Personalverwaltung	☐ Authentifizierungsdaten
☐ Vertragsdaten	☐ Gesundheitsdaten	☐
☐ Transaktionsdaten	☐ Stammdaten	☐

3. Kreis der von der Datenerhebung, -verarbeitung oder –nutzung Betroffenen*

☐ Kunden	☐ Mitarbeiter	☐ Angehörige
☐ Nutzer	☐ Auszubildende	☐ Unterhaltsberechtigte
☐ Interessenten	☐ Bewerber	☐ Ruheständler
☐ Kontaktpersonen	☐ Praktikanten	☐ Pressevertreter
☐ Lieferanten / Dienstleister	☐ frühere Mitarbeiter	☐ Geschädigte
☐ Geschäftspartner	☐ Berater	☐ Zeugen
☐ Gesellschafter	☐ Mitglieder	☐
☐ Makler / Vermittler	☐ Mieter	☐

* vom Auftraggeber auszufüllen

Anlage 2 - Darstellung der technischen und organisatorischen Maßnahmen gemäß §§ 11, 9 BDSG und Anlage

In diesem Dokument beschreiben wir die wesentlichen technischen und organisatorischen Sicherheitsmaßnahmen, die wir zum Schutz Ihrer Daten ergreifen. Aus Sicherheitsgründen geben wir nur eine allgemeine Beschreibung, denn der beste Schutz Ihrer Daten ist die Geheimhaltung der genauen Sicherheitsmaßnahmen. Soweit erforderlich, sinnvoll und wirtschaftlich werden die wesentlichen Systeme mit den beschriebenen Maßnahmen ganz oder teilweise ausgestattet. Die Sicherheit und Verfügbarkeit der STRATO Rechenzentren wird vom TÜV Süd regelmäßig nach DIN ISO 27001 geprüft. Datenschutz und Datensicherheit sind für uns von zentraler Bedeutung. Die Sicherheitsmaßnahmen werden kontinuierlich an den technischen Fortschritt und die aktuellen Gefährdungsszenarien angepasst.

1. Zutrittskontrolle

Unsere Rechenzentrumsgebäude sind durch Sicherheitsschlösser, vergitterte Fenster und Rollos gesichert. Der Zutritt über die vorgesehenen Zutrittswege ist nur autorisierten Personen mit Magnetkarte und Schlüssel möglich. Darüber hinaus sind die Zutrittswege durch Wachschutz, Video- und Alarmanlagen gesichert. Zutrittsberechtigte Mitarbeiter sind organisatorisch festgelegt, Magnetkarten und Schlüssel werden nur entsprechend der Organisationsanweisung vergeben. Über den Zutritt werden Anwesenheitslisten geführt, Regelungen für Fremdpersonal und Richtlinien zur Begleitung von Gästen sind vorhanden.

2. Zugangskontrolle

Der Zugang zu Systemen erfolgt mit Authentifizierung durch individuelle Benutzerkennung und Passwort. Berechtigungen werden nach einem Zugangsberechtigungskonzept vergeben, die Passwörter müssen den Sicherheitsanforderungen nach ISO 27001 genügen. Die Systeme sind gegen unberechtigten Zugang z.B. durch eine Firewall gesichert.

Bei Root-Servern haben unsere Mitarbeiter keinerlei Zugang. Dementsprechend obliegt es dem Kunden, das System zu sichern.

3. Zugriffskontrolle

Berechtigungen sind in den IT-Systemen festgelegt, differenzierte Zugriffe und differenzierte Berechtigungen werden festgelegt. Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch) sind getrennt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewahrt. Test- und Produktionsumgebung sind getrennt. Fernwartungen werden mit eindeutiger Benutzerkennung vorgenommen und protokolliert.

Bei Root-Servern haben unsere Mitarbeiter keinerlei Zugriffsmöglichkeit.

4. Weitergabekontrolle

Alle unsere Mitarbeiter werden auf das Datengeheimnis nach § 5 BSDG verpflichtet. Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt, Daten verschlüsselt und Schnittstellen gegen unbefugten Datenexport gesichert.

5. Eingabekontrolle

Die Daten werden vom Auftraggeber selbst eingegeben. Unsere Mitarbeiter dürfen grundsätzlich nicht auf Ihre Daten zugreifen bzw. Daten eingeben, verändern oder löschen. Bei Root-Servern haben unsere Mitarbeiter keinerlei Zugriffsmöglichkeit. Wir nehmen Sperrungen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges vor. Die Vornahme von Sperrungen wird protokolliert. Die Protokolldaten werden aufbewahrt und enthalten die Mitarbeiterkennung. Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

6. Auftragskontrolle

Wir schließen auf Wunsch einen schriftlichen Vertrag, der den Datenverarbeitungszweck regelt und ein Weisungsrecht enthält. Unsere Mitarbeitern kennen den Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten.
Ein IT-Organisationshandbuch / IT-Sicherheitskonzept ist vorhanden. Unterauftragsverhältnisse werden schriftlich beauftragt.

7. Verfügbarkeitskontrolle

Die Rechenzentren verfügen über eine unterbrechungsfreie Stromversorgung durch Batterien und Dieselaggregate. Die Primärtechnik und die wesentliche Sekundärtechnik ist redundant aufgebaut. Backups werden regelmäßig erstellt und die Daten auf getrennten Systemen gespiegelt, soweit dies Leistungsbestandteil ist. Bei Root-Servern erfolgen Backup und Datensicherung nicht durch uns, weil wir keinen Zugriff auf die Daten haben. Wiederherstellungsmöglichkeiten bei Datenverlust sind vorgesehen. Brandmeldeanlagen, Löschanlagen mit Löschgas und ein Notfallplan für die verschiedenen Gefährdungsszenarien sorgen für den physikalischen Schutz Ihrer Daten.

8. Trennungskontrolle

Je nach Paket werden Ihre Daten physikalisch oder logisch / virtuell von anderen Daten getrennt. Die Datensicherung erfolgt auf physikalisch oder virtuell getrennten Einheiten.