Die aktuellste Version dieser Informationen finden Sie unter staffbase.com.

Staffbase Auftragsverarbeitungsvertrag

Dies ist eine archivierte Version des Staffbase Auftragsverarbeitungsvertrags. Sehen Sie sich die aktuelle Version ([URL: https://staffbase.com/de/legal/dpa/](https://staffbase.com/de/legal/dpa/)) oder frühere Versionen ([URL: https://staffbase.com/en/legal/dpa/archive/](https://staffbase.com/en/legal/dpa/archive/)) an.

19. März 2020

Dieser Staffbase Auftragsverarbeitungsvertrag („**AVV**“) ist Teil der Staffbase Nutzungsbedingungen ([URL: https://staffbase.com/de/agb/](https://staffbase.com/de/agb/)) („**Vereinbarung**“). Im Falle eines Widerspruchs zwischen der Vereinbarung und dem AVV hat der AVV Vorrang.

1 DEFINITIONEN.

- 1.1 „Aufsichtsbehörde“** bedeutet jede unabhängige Behörde, die für die Überwachung der Anwendung des Anwendbaren Datenschutzrechts zuständig ist.
- 1.2 „Anwendbares Datenschutzrecht“** bedeutet alle anwendbaren Gesetze und Vorschriften in Bezug auf den Datenschutz und die Privatsphäre, denen der Kunde unterliegt und die für die Verarbeitung Personenbezogener Daten im Rahmen der Vereinbarung gelten. Anwendbares Datenschutzrecht beinhaltet: (i) EU-Datenschutzrecht; (ii) in Bezug auf das Vereinigte Königreich alle anwendbaren nationalen Gesetze, die die DSGVO ersetzen oder in nationales Recht umsetzen oder alle anderen Gesetze in Bezug auf Datenschutz und Privatsphäre infolge des Austritts des Vereinigten Königreichs aus der Europäischen Union; und (iii) das Schweizer Bundesgesetz über den Datenschutz vom 19. Juni 1992 sowie die Verordnung zum Bundesgesetz über den Datenschutz; jeweils in der geänderten, aufgehobenen, abgelösten oder ersetzten Fassung.

- 1.3 „EU-Datenschutzrecht“** bedeutet alle für die Europäische Union („EU“), den Europäischen Wirtschaftsraum („EWR“) und für die Mitgliedstaaten der Vorgenannten geltenden Datenschutzgesetze und -vorschriften, einschließlich (i) die Verordnung 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („**DSGVO**“); (ii) die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, geändert durch die Richtlinie 2009/136/EG; und (iii) die anwendbaren nationalen Umsetzungen von (i) und (ii) in den EU- und EWR-Mitgliedsstaaten.
- 1.4 „Modellklauseln“** sind die Standardvertragsklauseln für Auftragsverarbeiter, die gemäß dem Beschluss 2010/87/EU der Europäischen Kommission vom 5. Februar 2010 genehmigt wurden, oder alle aktualisierten Standardvertragsklauseln, die von der Europäischen Kommission genehmigt wurden.
- 1.5 „Personenbezogene Daten“** sind alle Kundendaten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, soweit diese Informationen durch das Anwendbare Datenschutzrecht geschützt sind. Personenbezogene Daten umfassen unter anderem die in **Anlage 1** beschriebenen Personenbezogenen Daten.
- 1.6 „Unterauftragsverarbeiter“** bezeichnet jeden Auftragsverarbeiter, der von Staffbase oder von Verbundenen Unternehmen von Staffbase beauftragt wurde, um bei der Erfüllung der Verpflichtungen von Staffbase im Rahmen der Vereinbarung zu unterstützen. Zu den Unterauftragsverarbeitern können auch Dritte oder Verbundene Unternehmen von Staffbase gehören. Die Unterauftragsverarbeiter sind in **Anlage 2** aufgeführt.
- 1.7 „Verbundenes Unternehmen“** hat die gleiche Bedeutung wie in der Vereinbarung.
- 1.8 „Verletzung des Schutzes Personenbezogener Daten“** bedeutet eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum unbefugten Zugriff auf Personenbezogene Daten geführt hat, die von Staffbase und/oder den Unterauftragsverarbeitern von Staffbase im Zusammenhang mit der Bereitstellung der Staffbase-Dienste übertragen, gespeichert oder anderweitig verarbeitet wurden.

1.9 „Weisungen“ sind die schriftlichen Weisungen des Kunden an Staffbase für die Verarbeitung Personenbezogener Daten, bestehend aus der Vereinbarung, allen Bestellungen, allen Weisungen, die der Kunde über die Nutzung der Staffbase-Dienste erteilt, sowie allen zusätzlichen Weisungen, die von den Parteien einvernehmlich schriftlich vereinbart wurden.

Die Begriffe **„Verantwortlicher“**, **„Betroffene Person“**, **„Auftragsverarbeiter“** und **„Verarbeitung“** haben die Bedeutung, die ihnen nach dem EU-Datenschutzrecht zukommt, und **„verarbeiten“**, **„verarbeitet“** und **„verarbeitete“** werden entsprechend ausgelegt. Alle anderen Begriffe, die in diesem AVV nicht explizit definiert sind, haben die gleiche Bedeutung wie in der Vereinbarung.

2 ROLLEN UND VERANTWORTLICHKEITEN.

2.1 Rollen der Parteien. Die Parteien verstehen und vereinbaren, dass in Bezug auf die Verarbeitung Personenbezogener Daten der Kunde der Verantwortliche und Staffbase der Auftragsverarbeiter ist. Staffbase oder die Verbundenen Unternehmen von Staffbase können Unterauftragsverarbeiter nach Maßgabe der in diesem AVV festgelegten Anforderungen beauftragen. Die Einzelheiten der Verarbeitung werden in **Anlage 1** erläutert.

2.2 Verarbeitung durch den Kunden. Der Kunde verarbeitet Personenbezogene Daten in Übereinstimmung mit den Anwendbaren Datenschutzrecht und stellt sicher, dass seine Weisungen auch Anwendbares Datenschutzrecht einhalten. Zwischen den Parteien hat der Kunde die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der Personenbezogenen Daten und die Methoden, mit denen er die Personenbezogenen Daten erfasst.

2.3 Verarbeitung durch Staffbase. Staffbase verarbeitet Personenbezogene Daten nur wie in diesem AVV, der Vereinbarung, allen relevanten Bestellungen und allen anderen schriftlichen Weisungen des Kunden beschrieben (**„Zweck“**). Staffbase wird die Personenbezogene Daten nicht für andere Zwecke verarbeiten, es sei denn: (i) dies ist mit dem Kunden schriftlich vereinbart; oder (ii) dies ist nach geltendem Recht erforderlich. Staffbase wird den Kunden unverzüglich informieren, wenn nach Ansicht von Staffbase eine Weisung gegen Anwendbares Datenschutzrecht verstößt. In diesem Fall behält sich Staffbase das Recht vor, die Ausführung der Weisungen zu verweigern und/oder auszusetzen.

3 ANTRÄGE UND KONSULTATION.

3.1 Anträge Betroffener Personen. Unter Berücksichtigung der Art der Verarbeitung wird Staffbase den Kunden in angemessener Weise unterstützen, damit der Kunde seinen Verpflichtungen gegenüber den Rechten der Betroffenen Personen gemäß dem Anwendbaren Datenschutzrecht nachkommen kann. Zu den Rechten der Betroffenen Person gehören unter anderem: Auskunftsrecht, Recht auf Berichtigung, Recht auf Einschränkung der Verarbeitung, Recht auf Löschung („Recht auf Vergessenwerden“), Widerspruchsrecht oder Recht auf Datenübertragbarkeit (jeweils ein „**Antrag der Betroffenen Person**“). Wenn ein Antrag der Betroffenen Person direkt an Staffbase gestellt wird, wird Staffbase den Kunden, soweit gesetzlich zulässig, umgehend informieren. Staffbase wird ohne vorherige Zustimmung des Kunden nicht direkt auf einen Antrag der Betroffenen Person antworten, es sei denn, dies ist angemessen, z.B. um die Betroffene Person an den Kunden zu verweisen. Der Kunde ist allein verantwortlich für die Beantwortung von Anträgen der Betroffenen Person.

3.2 DSFA. Auf Anfrage des Kunden und in dem nach Anwendbarem Datenschutzrecht erforderlichen Umfang leistet Staffbase dem Kunden angemessene Zusammenarbeit und Unterstützung bei der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) bezogen auf die Nutzung der Staffbase-Dienste durch den Kunden.

3.3 Konsultierung der Aufsichtsbehörde. Soweit nach dem Anwendbaren Datenschutzrecht erforderlich, leistet Staffbase dem Kunden angemessene Unterstützung bei der Zusammenarbeit oder der vorherigen Konsultation mit einer Aufsichtsbehörde.

4 SICHERHEIT UND VERTRAULICHKEIT.

4.1 Personal. Staffbase stellt sicher, dass die Mitarbeiter von Staffbase sowie die Mitarbeiter der Verbundenen Unternehmen von Staffbase sowie externe Dienstleister, die Zugang zu Personenbezogenen Daten haben: (i) einer schriftlichen Verpflichtung unterliegen, Personenbezogene Daten vertraulich zu behandeln; und (ii) in angemessener Weise in den sorgfältigen Umgang mit Personenbezogenen Daten eingewiesen werden. Staffbase wird Maßnahmen zur Beschränkung des Zugangs der Mitarbeiter zu Personenbezogenen Daten gemäß den Sicherheitsmaßnahmen durchführen.

4.2 Sicherheitsmaßnahmen. Unter Berücksichtigung des Standes der Technik, der Kosten der Implementierung und der Art, des Umfangs, des Kontexts und des Zwecks der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten der Betroffenen

Person wird Staffbase geeignete technische und organisatorische Maßnahmen, wie in Anlage 3 dieses AVVs („**Sicherheitsmaßnahmen**“) beschrieben, implementieren und aufrechterhalten, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Staffbase überwacht regelmäßig die Einhaltung seiner Sicherheitsmaßnahmen. Staffbase kann von Zeit zu Zeit alternative angemessene Sicherheitsmaßnahmen implementieren und dabei sicherstellen, dass das Sicherheitsniveau der definierten Maßnahmen nicht verringert wird.

5 VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN.

5.1 Meldung. Sobald Staffbase von einer Verletzung des Schutzes

Personenbezogener Daten Kenntnis erlangt, wird Staffbase diese dem Kunden unverzüglich melden und wird bei der Ermittlung der Ursache der Verletzung des Schutzes Personenbezogener Daten in wirtschaftlich angemessener Weise kooperieren und Unterstützung leisten. Die Meldung muss, soweit verfügbar, Folgendes umfassen: (i) eine Beschreibung was geschehen ist; (ii) den Umfang der Verletzung des Schutzes Personenbezogener Daten, einschließlich einer Beschreibung der Art der betroffenen Personenbezogenen Daten; (iii) eine Beschreibung der Reaktion von Staffbase; und (iv) andere Informationen, deren Offenlegung gemäß Anwendbarem Datenschutzrecht in angemessener Weise verlangt werden kann. Staffbase stellt dem Kunden Informationen zur Verfügung, die für die Erfüllung der Melde- und Kommunikationspflichten des Kunden erforderlich sind, soweit diese Informationen Staffbase wirtschaftlich angemessen zur Verfügung stehen. Die Verpflichtung von Staffbase, eine Verletzung des Schutzes Personenbezogener Daten gemäß dieser Ziffer zu melden oder darauf zu reagieren, stellt kein Schuldanerkenntnis oder eine Anerkenntnis der Haftbarkeit seitens Staffbase in Bezug auf die Verletzung des Schutzes Personenbezogener Daten dar.

5.2 Kooperation. Außerdem wird Staffbase wirtschaftlich angemessene Maßnahmen ergreifen, um die Auswirkungen der Verletzung des Schutzes Personenbezogener Daten zu beheben oder zu mindern, soweit dies in der Kontrolle von Staffbase liegt. Staffbase kann seine Mitteilungen verzögern, wenn dies von Verfolgungsbehörden verlangt wird oder wenn es legitimerweise notwendig ist, um eine Verletzung des Schutzes Personenbezogener Daten zu untersuchen oder zu beheben. Aus Sicherheitsgründen verpflichten sich die Parteien, Informationen über eine Verletzung des Schutzes Personenbezogener Daten vertraulich zu behandeln, es sei denn, eine Offenlegung ist gesetzlich vorgeschrieben.

6 UNTERAUFTRAGSVERARBEITER.

6.1 Einschaltung von Unterauftragverarbeitern. Der Kunde stimmt der Verwendung der in **Anlage 2** aufgeführten Unterauftragsverarbeiter durch Staffbase zu. Staffbase ist berechtigt, zusätzliche Unterauftragsverarbeiter einzuschalten oder Unterauftragsverarbeiter zu ersetzen, vorausgesetzt, Staffbase informiert den Kunden über die Identität des Unterauftragsverarbeiter und den Umfang der geplanten Verarbeitung. Staffbase wird mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung mit Datenschutzpflichten eingehen, die mindestens das gleiche Schutzniveau enthalten wie die in diesem AVV, soweit dies auf die Art der vom Unterauftragsverarbeiter erbrachten Dienstleistungen anwendbar ist. Der Kunde erkennt an, dass er den Staffbase-Dienst zusammen mit Drittanbieterdiensten nutzen kann und dass diese Produkte keine Unterauftragsverarbeiter von Staffbase sind.

6.2 Einspruch gegen Unterauftragsverarbeiter. Der Kunde kann gegen die Einschaltung eines neuen Unterauftragsverarbeiters durch Staffbase innerhalb von 30 Kalendertagen nach Erhalt der Mitteilung von Staffbase gemäß Ziffer 6.1 schriftlich Einspruch erheben. Wenn der Kunde Einspruch erhebt, wird er Staffbase schriftlich über die angemessenen datenschutzrechtlichen Gründe für den Einspruch informieren. Die Parteien vereinbaren, die Bedenken des Kunden nach Treu und Glauben zu erörtern, um eine wirtschaftlich angemessene Lösung zu erreichen.

6.3 Nicht-EWR-Unterauftragsverarbeiter. Staffbase übermittelt keine Personenbezogenen Daten in Länder außerhalb des EWRs, es sei denn, Staffbase hat angemessene Maßnahmen ergriffen, um sicherzustellen, dass die Übermittlung mit EU-Datenschutzrecht vereinbar ist. Solche Maßnahmen können unter anderem die Übermittlung Personenbezogener Daten: (i) an einen Unterauftragsverarbeiter in einem Land, dem die Europäische Kommission per Angemessenheitsbeschluss ein angemessenes Datenschutzniveau bestätigt hat; oder (ii) auf der Grundlage von Modellklauseln, umfassen. In Bezug auf Modellklauseln ermächtigt der Kunde Staffbase, bei Bedarf Modellklauseln mit einem Unterauftragsverarbeiter für die Verarbeitung der relevanten Personenbezogenen Daten abzuschließen.

7 ÜBERPRÜFUNGEN.

7.1 Durch den Kunden. Staffbase stellt dem Kunden alle relevanten Informationen zur Verfügung, die sich im Besitz oder unter der Kontrolle von Staffbase befinden und die erforderlich sind, um die Einhaltung dieses AVVs

nachzuweisen. Staffbase wird auch Überprüfungen, einschließlich Inspektionen, durch den Kunden (oder durch von ihm beauftragte externe Prüfer) im Zusammenhang mit der Verarbeitung Personenbezogener Daten durch Staffbase ermöglichen und zu diesen beitragen. Der Kunde erklärt sich bereit, alle angemessenen Maßnahmen zu ergreifen, um unnötige Störungen des Betriebs von Staffbase zu verhindern, und seine Prüfungsrechte nur einmal alle zwölf (12) Kalendermonate auszuüben, außer, wenn: (i) und soweit dies auf Anweisung einer Aufsichtsbehörde erforderlich ist; (ii) der Kunde glaubt, dass eine weitere Überprüfung aufgrund einer Verletzung des Schutzes Personenbezogener Daten erforderlich ist, oder (iii) der Kunde dokumentierte sachliche Gründe für den Verdacht vorlegen kann, dass Staffbase wesentliche Verpflichtungen dieses AVVs verletzt hat. Die Kosten der Überprüfung, einschließlich aller angemessenen Kosten, die Staffbase für die Zusammenarbeit mit der Überprüfung aufbringen muss, werden vom Kunden getragen. Jeder externe Prüfer muss entsprechend qualifiziert sein und vor jeder Überprüfung eine entsprechende Geheimhaltungs- und Vertraulichkeitsvereinbarung mit Staffbase unterzeichnen.

7.2 Durch Aufsichtsbehörden. Staffbase gewährt dem Kunden oder einer Aufsichtsbehörde angemessenen Zugang zur Dokumentation und den Systemen von Staffbase im Falle einer von einer Aufsichtsbehörde geforderten Überprüfung, soweit die Überprüfung für die Einhaltung des Anwendbaren Datenschutzrechts erforderlich ist. Die Parteien werden sich einvernehmlich über den Zeitpunkt und den Umfang dieser Überprüfungen einigen, die: (i) in einer solchen Weise durchgeführt werden, dass sie Unterbrechungen des Geschäftsbetriebs von Staffbase minimieren; und (ii) auf alleinige Kosten des Kunden durchgeführt werden.

7.3 Vertrauliche Informationen von Staffbase. Alle Zusammenfassungen, Prüfungsberichte oder andere Prüfungsergebnisse werden als Vertrauliche Informationen von Staffbase betrachtet und unterliegen dem Abschnitt „Vertrauliche Informationen“ der Vereinbarung. Staffbase ist nicht verpflichtet, Geschäftsgeheimnisse, einschließlich Algorithmen, Quellcode, Betriebsgeheimnisse und ähnliche Informationen offenzulegen.

8 BEENDIGUNG UND LÖSCHUNG.

8.1 Rückgabe oder Löschung Personenbezogener Daten. Nach Ablauf der Abonnementdauer oder der Beendigung der Vereinbarung wird Staffbase alle im Rahmen dieses AVVs verarbeiteten Personenbezogenen Daten löschen oder zurückgeben. Diese Anforderung gilt nicht, soweit Staffbase nach geltendem

Recht verpflichtet ist, einige oder alle Personenbezogenen Daten aufzubewahren.

8.2 Speicherung der Dokumentation. Staffbase kann nach Beendigung der Vereinbarung eine Dokumentation zum Nachweis der Einhaltung ihrer Verpflichtungen im Rahmen dieses AVVs behalten.

9 ALLGEMEINES. Wenn der Kunde und Staffbase einen vorherigen Auftragsverarbeitungsvertrag unterzeichnet haben, wird dieser hiermit beendet und durch diesen AVV zum Datum der letzten Unterschrift der letzten Bestellung ersetzt. Wenn eines der Verbundenen Unternehmen des Kunden als Verantwortlicher (entweder allein oder zusammen mit dem Kunden) hinsichtlich der Verarbeitung Personenbezogener Daten angesehen wird, ist der Kunde gemäß diesem AVV für diese Personenbezogenen Daten und für dieses Verbundene Unternehmen verantwortlich. Dieser AVV ist als Anlage zur Vereinbarung Teil der Vereinbarung und unterliegt allen Bedingungen und Bestimmungen, einschließlich der Regelungen der Vereinbarung hinsichtlich Haftungsbeschränkungen, Kündigung/Beendigung, Gerichtsbarkeit und geltendem Recht.

Anlage 1 – Personenbezogene Daten

A. Art und Zweck der Verarbeitung.

Staffbase verarbeitet Personenbezogene Daten, soweit dies für die Erbringung der Staffbase-Dienste gemäß der Vereinbarung erforderlich ist, wie in der Bestellung näher erläutert wird, und nach näherer Weisung des Kunden bei seiner Nutzung der Staffbase-Dienste.

B. Dauer der Verarbeitung.

Vorbehaltlich Ziffer 9 des AVVs verarbeitet Staffbase Personenbezogene Daten für die Dauer der Vereinbarung, es sofern nicht schriftlich etwas anderes vereinbart wurde.

C. Kategorien Betroffener Personen.

Die übermittelten Personenbezogenen Daten betreffen die folgenden Kategorien Betroffener Personen:

x	Registrierte Nutzer: Nutzer, die vom Kunden speziell benannt und autorisiert werden, auf den Staffbase-Dienst zuzugreifen.
x	Nicht Registrierte Nutzer: Nutzer, die auf den Öffentlichen Bereich zugreifen und keine Admin-Nutzer oder Registrierten Nutzer sind.

D. Kategorien Personenbezogener Daten.

Der Kunde kann Personenbezogene Daten an die Staffbase-Dienste übermitteln, deren Umfang vom Kunden bestimmt und kontrolliert wird und die möglicherweise Folgendes enthalten:

x	Profilinformationen: Profilinformationen des Nutzers, wie z.B. Name, E-mail-Adresse, Position, Abteilung und Standort sowie weitere erforderlichen oder freiwilligen Profilinformationen.
x	Login-Daten: E-Mail and Passwort.
x	Inhalte: Alle anderen Personenbezogenen Daten, die in den Kundendaten enthalten sind, z.B. Personenbezogene Daten in Chats oder Mediendateien.
x	Technische Informationen: Gerätetyp, IP-Adresse, User-ID, Betriebssystem, Browser-Typ, User-Agent, Zeitstempel der Besuche und lokale Speicherung.

E. Besondere Kategorien Personenbezogener Daten (falls zutreffend).

Der Kunde darf die Staffbase-Dienste nicht zur Verarbeitung besonderer Kategorien Personenbezogener Daten nutzen, es sei denn, dies ist durch die Vereinbarung oder die Servicespezifischen Bedingungen ausdrücklich gestattet.

Anlage 2 - Unterauftragsverarbeiter

Liste der genehmigten Unterauftragsverarbeiter gemäß Ziffer 6:

Diese Anlage enthält eine Liste der aktuellen Unterauftragsverarbeiter, die mit der Verarbeitung Personenbezogener Daten in dem unten genannten Umfang beauftragt sind. Der Verantwortliche stimmt der Beauftragung dieser Unterauftragsverarbeiter zu, die von Zeit zu Zeit gemäß den Bedingungen in Ziffer 6 geändert werden können.

Dienstleister	Land und Adresse	Verarbeitungstätigkeiten	Speicherort
Infrastruktur – DE Hosting			

1&1 IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	ISO 27001 zertifiziertes Datenhosting.	Deutschland
SysEleven GmbH	Boxhagener Straße 80, 10245 Berlin, Deutschland	ISO 27001 zertifiziertes Datenhosting.	Deutschland
Infrastruktur – US Hosting			
<i>Zusätzlich zu den oben genannten Unterauftragsverarbeitern verwenden wir den folgenden Unterauftragsverarbeiter für Kunden mit US Hosting</i>			
Microsoft Corporation (Azure)	One Microsoft Way Redmond, Washington 98052, USA	ISO 27001 zertifiziertes Datenhosting.	USA
Weitere Staffbase-Dienste Funktionen			
Mailjet SAS	13-13 bis, rue de l'Aubrac – 75012 Paris, Frankreich	ISO 27001 zertifizierter E-Mail-Dienstleister, der für die Versendung von E-Mails an Autorisierte Nutzer verwendet wird. Mailjet hat Zugriff auf die E-Mail-Adressen der Autorisierte Nutzer und den Inhalt der E-Mail selbst.	EU
Zendesk, Inc.	1019 Market Street, San Francisco, CA 94103, USA	Zendesk stellt eine Plattform zur Verwaltung von Kundensupportanfragen bereit. Nur Admin-Nutzer können über die Zendesk-Plattform Support von Staffbase anfordern. Die Personenbezogenen Daten, die von Zendesk in dieser Hinsicht verarbeitet werden können, sind der Name des Admin-Nutzers, seine E-Mail-Adresse und der Inhalt des Support-Tickets.	EU
Optionale Unterauftragsverarbeiter			
Amazon Web Services Inc.*	410 Terry Avenue North, Seattle, Washington 98109-5210, USA	Amazon stellt ein Content Delivery Network (CDN) zur internationalen Bereitstellung von Media Assets (Bilder, Videos, Dateien), die zur Verwendung mit dem Staffbase-Dienst ausgewählt sind, bereit. Die Nutzung des CDN durch den Kunden führt zu einer schnelleren Lieferung von Mediendateien. Vom Kunden hochgeladene Mediendateien können Personenbezogene Daten wie Namen oder Bilder enthalten. *Wenn der CDN-Dienst deaktiviert ist, ist Amazon Web Services Inc. kein Unterauftragsverarbeiter.	Global
Microsoft Corporation*	One Microsoft Way Redmond, Washington 98052, USA	ISO 27001-zertifizierter Übersetzungsdienst. Wir verwenden Microsoft Translator, um On-Demand Übersetzungen zu erstellen. Microsoft kann Personenbezogene Daten, die im Inhalt der zur Übersetzung gesendeten Dokumente gespeichert sind, verarbeiten. Microsoft löscht diese Informationen sofort, so dass keine Übersetzungen in den permanenten Speicher geschrieben werden. Es wird keine Aufzeichnung des eingereichten Inhalts oder eines Teils davon in Microsoft-Rechenzentren vorgenommen. *Wenn der Übersetzungs-Dienst deaktiviert ist oder für den Endnutzer nicht verfügbar ist, ist Microsoft Corporation kein Unterauftragsverarbeiter.	EU

Staffbase Gruppe

Abhängig vom geografischen Standort eines Kunden oder seiner Admin-Nutzer und der Art der bereitgestellten Staffbase-Dienste kann Staffbase beim Zugriff auf Kundendaten auch einen oder mehrere der folgenden Verbundenen Unternehmen von Staffbase als Unterauftragsverarbeiter beauftragen:

Verbundene Unternehmen von Staffbase	Informationen zu den Verbundenen Unternehmen
Staffbase UK Ltd	UK – Registriert in England unter der Nummer 11666265
Staffbase B.V.	Niederlande – Registriert in den Niederlanden unter der Nummer 75849895

Diese Verbundenen Unternehmen von Staffbase können für einen Kunden (Kunden-)Support und ähnliche Dienstleistungen erbringen. Zum Beispiel kann es sein, dass unser Customer Support Team von Staffbase Inc. einem Kunden, der die Vereinbarung mit der Staffbase GmbH abgeschlossen hat, Support leisten muss. Staffbase hat einen gruppeninternen Auftragsverarbeitungsvertrag, einschließlich Standardvertragsklauseln, um diese Übermittlungen zu erleichtern

Anlage 3 – Technische und Organisatorische Maßnahmen (TOMs)

1. VERTRAULICHKEIT.

Zutrittskontrolle.

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

Das Hosting der Applikation erfolgt außerhalb der Hoheit von Staffbase durch die Unterauftragsverarbeiter, wie in **Anlage 2** aufgeführt.

Die Arbeitsplatzrechner der Staffbase befinden sich in abgeschlossenen Büros. Zugang zu den Büros haben nur die Mitarbeiter und der Reinigungsdienst. Nur Mitarbeiter sowie der Reinigungsdienst erhalten Zugangsmedien (Schlüssel, Keycard o.ä.). Gäste werden an der Tür in Empfang genommen und zum Ansprechpartner begleitet.

Die Ausgabe und Rücknahme der Zugangsmedien wird schriftlich protokolliert. Mit dem Reinigungsdienstleister besteht eine Sicherheitsvereinbarung.

Zugangskontrolle.

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

Der Zugang zur DV-Anlage ist erst nach Identifikation und erfolgreicher Authentisierung durch Benutzername und Passwort der befugten Personen durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen möglich. Der Zugang wird bei fehlender Berechtigung entsprechend verwehrt.

Der Kreis der Personen, die befugt Zugang zu DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum beschränkt. Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu DV-Anlagen werden auf 3rd und 2nd Level Ebene grundsätzlich nur personengebunden vergeben und sind an ein persönliches Credential (Passwort) geknüpft (Benutzerkennung). Authentifizierungsmedien und/oder Benutzerkennung/Passwort-Kombination werden nicht an Dritte weitergegeben.

Zugänge für temporär beschäftigte Personen (Externe Entwickler, Praktikanten, Auszubildende) werden individuell vergeben. Es werden keine wiederverwendbaren Kennungen (z.B. Azubi1, etc.) vergeben.

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist eingerichtet, dokumentiert und wird angewendet. Automatische Zugangssperre: Bei mehr als fünf Minuten Inaktivität der Arbeitsstation bzw. des Terminals wird ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert.

Manuelle Zugangssperre: Arbeitsstationen und Terminals werden bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung geschützt (durch manuelle Aktivierung des kennwortgeschützten Bildschirmschoners oder durch Sperrung des Systems).

Passwörter werden mittels Passwortmanager verwaltet und werden mit einer minimalen Komplexität von mindestens 32 Zeichen sowie einem Zeichenmix aus Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben generiert.

Der Zugang zu den Arbeitsstationen sowie zum Passwortmanager wird durch ein Passwort geschützt. Das Passwort muss aus mindestens 10 Zeichen bestehen.

Zugriffskontrolle.

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

Zugriff auf Daten des Kunden haben ausgewählte Mitarbeiter von Staffbase in folgenden Rollen:

- 3rd Level – Systemadmin: personengebundener Zugriff auf alle Daten innerhalb der zugehörigen Kundeninstanz inkl. Datenbank.
- 2nd Level – Supportadmin: personengebundener Zugriff auf alle Daten innerhalb der zugehörigen Kundeninstanz, aber keinen Server/Datenbankzugriff.
- 1st Level – Customer Success Zugang: Zugriff auf alle Daten innerhalb einer Kundeninstanz über die Applikation entsprechend der Freigabe durch den Kunden. Dieser legt auf Applikationsebene die Rechte des Accounts fest (App-Admin, Redakteur, Nutzer etc.). Kein Zugriff auf Datenbanken sowie Login-Daten (E-Mail und Passwort) der einzelnen Nutzer möglich. Dieser Supportzugang ist nicht personengebunden und steht prinzipiell allen Mitarbeitern des Customer Success/Support Teams zur Verfügung.

Die Rollen haben ausschließlich den minimal notwendigen Kreis von Mitarbeitern der Staffbase. Die Vergabe der Zugänge wird protokolliert und mindestens jährlich überprüft.

Trennungskontrolle.

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

Es erfolgt eine Trennung von Test- und Produktionsdaten sowie eine Trennung von Entwicklungs-, Staging- und Produktionsinstanzen.

Pseudonymisierung & Verschlüsselung.

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.

Verschlüsselung: Sämtliche Kommunikation zwischen Server und Clients wird nach dem Stand der Technik verschlüsselt.

Pseudonymisierung: Bei ausgewählten Plugins ist zusätzlich eine Pseudonymisierung der Daten bei der Verarbeitung möglich.

2. INTEGRITÄT.

Weitergabekontrolle.

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

Daten werden ausschließlich unter Verwendung des verschlüsselten HTTPS Protokolls ausgetauscht.

Eingabekontrolle.

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

Es erfolgt eine Protokollierung von Zeitpunkt und Identität des Admin bei Anlage und Änderung von Nutzerdatensätzen.

3. VERFÜGBARKEIT UND BELASTBARKEIT.

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.

Staffbase stellt ein tägliches Backup der Daten sicher. Das Backup der Daten wird für 30 Tage aufbewahrt.

Schnelle Wiederherstellbarkeit.

Die Wiederherstellbarkeit des Backups im Notfall wird in jährlich durchgeführten Trainings erprobt und verbessert.

4. REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG.

Datenschutz-Management.

Staffbase hat für die Verarbeitung von Personenbezogenen Daten Prozesse und Arbeitsabläufe definiert. Die Kontrolle der Umsetzung findet regelmäßig durch den Datenschutzbeauftragten statt.

Schulung/Verpflichtung:

Alle Mitarbeiter bei Staffbase, die mit Personenbezogenen Daten umgehen, sind nachweislich zu folgenden Themenkomplexen unterwiesen:

- Grundsätze des Datenschutzes, einschließlich den technisch-organisatorischen Maßnahmen
- Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich Vorgängen des Kunden
- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen
- Fernmeldegeheimnis (Verpflichtung nach §88 TKG)
- Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes (schriftlich)

Die Unterweisung wird mindestens alle drei Jahre, bei Bedarf (z.B. Änderung der Auftragsumstände oder gesetzlicher Bestimmungen) jedoch auch in kürzeren Abständen, wiederholt.

Incident-Response-Management.

Staffbase informiert den Kunden ohne schuldhaftes Zögern über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Kunden. Staffbase wird diese unverzüglich beheben.

Datenschutzfreundliche Voreinstellungen.

Sparsamkeit bei der Datenerhebung: Es werden durch die Mitarbeiter-App nur solche Daten erhoben, gespeichert oder verarbeitet, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses mindestens notwendig sind.

Auftragskontrolle.

Weisungserteilung und -entgegennahme: Die auf Seiten von Staffbase zur Entgegennahme und Ausführung von Weisungen des Kunden befugten Personen sind durch Staffbase verbindlich spezifiziert. Im Regelfall handelt es sich um den Account Manager sowie die Mitarbeiter des Staffbase Customer Success/Support Teams.

Weisungen des Kunden werden grundsätzlich schriftlich entgegengenommen und bestätigt. Mündlich entgegengenommene Weisungen des Kunden müssen von diesem unverzüglich innerhalb von maximal 3 Werktagen schriftlich bestätigt werden.

Regelungen/Beschränkungen der Auftragsausführung: Es werden nur diejenigen Arbeiten durchgeführt, die in der Leistungsbeschreibung enthalten sind. Alle darüber hinausgehenden Arbeitsschritte müssen vorher dezidiert mit der zuständigen Stelle auf

Seiten des Kunden abgesprochen und schriftlich freigegeben werden. Staffbase stimmt den terminlichen Ablauf der Auftragsausführung vorab mit dem Kunden ab.

Copyright © 2015 to present, Staffbase (or its affiliates). All rights reserved.