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

Staffbase Auftragsverarbeitungsvertrag

21. November 2022

Dieser Staffbase Auftragsverarbeitungsvertrag (**„AVV“**) ist Bestandteil der Staffbase Nutzungsbedingungen (URL: https://staffbase.com/de/agb/) oder, falls zutreffend, Bestandteil des zwischen Staffbase und dem Kunden abgeschlossenen Master Subscription Agreement (die Staffbase Nutzungsbedingungen bzw. das Master Subscription Agreement jeweils die **„Anwendbare Vereinbarung“**). Im Falle eines Widerspruchs zwischen der Anwendbaren Vereinbarung und dem AVV ist der AVV maßgeblich

Die vorherige Version unseres Auftragsverarbeitungsvertrags finden Sie hier (URL: https://staffbase.com/de/legal/dpa/archive/v-20210817/).

1 DEFINITIONEN.

1.1 **„Aufsichtsbehörde“** bezeichnet jede unabhängige Behörde, die für die Überwachung der Anwendung des Anwendbaren Rechts zum Schutz der Privatsphäre zuständig ist.

1.2 **„Anwendbares Recht zum Schutz der Privatsphäre“** bedeutet Europäisches Datenschutzrecht.

1.3 **„Europäisches Datenschutzrecht“** bezeichnet **(i)** die Verordnung 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung) (**„DSGVO“**); **(ii)** anwendbare nationale Umsetzungsgesetze zur DSGVO Mitgliedstaaten der Europäische Union (**„EU“**), und des Europäischen Wirtschaftsraumes (**„EWR“**); **(iii)** das Datenschutzgesetz 2018, sowie die DSGVO soweit diese gemäß Abschnitt 3 des Aktes des

Vereinigten Königreichs zum Austritt aus der EU (European Union (Withdrawal) Act 2018) in das Recht des Vereinigten Königreichs (**"UK"**) übernommen worden ist, (**"UK Datenschutzrecht"**); **(iv)** 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; sowie **(v)** das Schweizer Bundesgesetz über den Datenschutz vom 19. Juni 1992 sowie die Verordnung zum Bundesgesetz über den Datenschutz (**"Schweizer DPA"**); in jedem der in (i) bis (v) bezeichneten Fälle in der aktualisierten, aufgehobenen, abgelösten oder ersetzten Fassung.

1.4 **„Modellklauseln"** bezeichnet die Standardvertragsklauseln für Auftragsverarbeiter, die gemäß dem Beschluss der Europäischen Kommission vom 4. Juni 2021 (EU) 2021/914 genehmigt wurden.

1.5 **„Personenbezogene Daten"** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, soweit diese Informationen durch das Anwendbare Recht zum Schutz der Privatsphäre geschützt sind. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person 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 auf https://staffbase.com/de/legal/unterauftragsverarbeiter/ (URL: https://staffbase.com/de/legal/unterauftragsverarbeiter/) (die **„Unterauftragsverarbeiter-Seite"**) 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 zu unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust oder Veränderung, zur unbefugten Offenlegung von

beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die von Staffbase und/oder den Unterauftragsverarbeitern von Staffbase im Zusammenhang mit der Bereitstellung der Staffbase-Dienste übermittelt, gespeichert oder auf sonstige Weise 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 Europäischen 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 Anwendbaren 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.** Wird Staffbase als Auftragsverarbeiter tätig, so verarbeitet Staffbase Personenbezogene Daten nur so wie in den dokumentierten Weisungen des Kunden, die in diesem AVV enthalten sind, der Anwendbaren Vereinbarung, den relevanten Bestellungen und sonstigen Weisungen 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)** Staffbase ist hierzu durch das Recht der Union oder der Mitgliedstaaten, dem Staffbase unterliegt, verpflichtet. In

letzterem Fall teilt Staffbase dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Staffbase wird den Kunden unverzüglich informieren, wenn nach Ansicht von Staffbase eine Weisung gegen Anwendbares Recht zum Schutz der Privatsphäre verstößt. In diesem Fall behält sich Staffbase das Recht vor, die Ausführung der Weisungen zu verweigern und/oder auszusetzen bis zu einer Bestätigung der Weisung durch den Kunden.

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 Vertrauliche Informationen. Staffbase wird alle Personenbezogene Daten als Vertrauliche Informationen behandeln, wie in der Anwendbaren Vereinbarung

festgelegt.

4.2 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.

4.3 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 2** 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 sowie alle Abhilfe- oder mildernden Maßnahmen, die von Staffbase ergriffen wurden oder geplant sind; und (iv) andere Informationen, deren Offenlegung gemäß Anwendbarem Recht zum Schutz der Privatsphäre 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 legitimer Weise 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 Unterauftragsverarbeitern. Der Kunde stimmt der Verwendung der auf der Unterauftragsverarbeiter-Seite 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. Staffbase wird den Kunden über einen neuen Unterauftragsverarbeiter informieren, bevor dieser Unterauftragsverarbeiter zur Verarbeitung Personenbezogener Daten in Verbindung mit den Staffbase-Diensten autorisiert wird. Soweit nach dem Anwendbaren Recht zum Schutz der Privatsphäre zulässig, kann der Kunde kann gegen die Einschaltung eines neuen Unterauftragsverarbeiters Einspruch erheben, jedoch ausschließlich aus vernünftigen Gründen, die sich auf den Datenschutz beziehen. Der Kunde wird Staffbase über seinen Einspruch

innerhalb von 30 Kalendertagen nach Mitteilung von Staffbase informieren. Der Einspruch des Kunden muss schriftlich (E-Mail ausreichend), unter Angabe der vernünftigen Gründe, die für den Einspruch sprechen, an privacy@staffbase.com (URL: mailto:privacy@staffbase.com) erfolgen. Die Parteien vereinbaren, die Bedenken des Kunden nach Treu und Glauben zu erörtern, um eine wirtschaftlich angemessene Lösung zu erreichen.

6.3 Nicht-Europäische-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 Europäischem-Datenschutzrecht vereinbar ist. Solche Maßnahmen liegen beispielsweise vor, bei der 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 und, soweit, sowie, nach Europäischem Datenschutzrecht erfordert, zusätzlicher Dokumentation.

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, es sei denn, Anwendbares Recht zum Schutz der Privatsphäre sieht eine anderweitige Kostenregelung vor. 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, soweit möglich, 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 können die folgenden Kategorien Betroffener Personen betreffen:

- Mitarbeiter des Kunden, die von diesem autorisiert worden sind, auf die Staffbase-Dienste zuzugreifen oder diese zu nutzen
- Berater / Auftragnehmer des Kunden, die von diesem autorisiert worden sind, auf die Staffbase-Dienste zuzugreifen oder diese zu nutzen
- andere Drittparteien, die vom Kunden autorisiert worden sind, auf die Staffbase-Dienste zuzugreifen oder diese zu nutzen
- im Hinblick auf Mitarbeiter E-Mail E-Mail-Empfänger
- im Hinblick auf Communications Control, Social Media Kontakts

D. Kategorien Personenbezogener Daten.

Die Kategorien der zu verarbeitenden personenbezogenen Daten hängen von dem spezifischen Produkt ab, welches vom Kunden gekauft oder verwendet wird. Der Kunde kann Personenbezogene Daten an die Staffbase-Dienste übermitteln, deren Umfang vom Kunden bestimmt und kontrolliert wird und die möglicherweise Folgendes enthalten:

Mitarbeiter App & Front Door Intranet
Profilinformationen: Profilinformationen des Nutzers, wie z.B. Name, E-Mail-Adresse, Position, Abteilung und Standort sowie weitere erforderliche oder freiwillige Profilinformationen.
Login-Daten: E-Mail-Adresse und Passwort.
Inhalte: Alle anderen Personenbezogenen Daten, die in den Kundendaten enthalten sind, z.B. Personenbezogene Daten in Chats oder Mediendateien.
Technische Informationen: Gerätetyp, IP-Adresse, Nutzer-ID, Betriebssystem, Browser-Typ, User-Agent, Zeitstempel der Besuche und lokale Speicherung.

Mitarbeiter E-Mail
Kontoinformationen: Vollständiger Name, E-Mail-Adresse und Passwort vom Autorisierten Nutzer.
E-Mail-Informationen: Vollständiger Name und E-Mail-Adresse von E-Mail-Empfängern, Namen von Verteilerlisten, die in die Felder „An“ und „CC“ eingegeben wurden, Inhalt von Vorlagen und Entwürfen für E-Mail-Newsletter sowie Betreffzeilen.
E-Mail-Metrikinformationen: Ungefährer Standort der E-Mail-Empfänger (wird verwendet, um Zeitzoneneinstellungen zu identifizieren und im Zusammenhang mit internen E-Mail-Metriken zu verwenden); Informationen über das Verhalten von E-Mail-Empfängern, einschließlich, aber nicht beschränkt auf das Lesen eines E-Mail-Newsletters oder das Anklicken eines Links in einem E-Mail-Newsletter, welche durch Tracking-Technologien wie Pixel und Cookies gesammelt werden; und alle optionalen Informationen zur Gruppierung, die vom Kunden hochgeladen werden, wie z.B. die Berufsbezeichnung, die Abteilung oder der Bürostandort.
Technische Informationen: Gerätetyp, IP-Adresse, Nutzer-ID, Betriebssystem, Browsertyp sowie Besuchs- und Nutzungsinformationen.

Communications Control
Kontoinformationen: Vollständiger Name, E-Mail-Adresse und Passwort vom Autorisierten Nutzer.
Social Media Unterhaltungen: @Handle des Social Media Accounts, Vollständiger Name des Social Media Kontakts, Inhalt der Nachricht und Unterhaltungshistorie.
Inhalt: sonstige Inhalte, die in den Kundendaten enthalten sind
Technische Informationen: Gerätetyp, IP-Adresse, Nutzer-ID, Betriebssystem, Browsertyp sowie Besuchs- und Nutzungsinformationen.

E. Besondere Kategorien Personenbezogener Daten (falls zutreffend).

Der Kunde darf die Staffbase-Dienste für die Verarbeitung besonderer Kategorien Personenbezogener Daten nur wie in den Servicespezifischen Bedingungen ausdrücklich erlaubt nutzen. Der Umfang besonderer Kategorien Personenbezogener Daten wird vom Kunden bestimmt und kontrolliert und kann die folgenden Kategorien betreffen:

- Rasse oder ethnische Herkunft;
- Politische Meinungen;
- Religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftszugehörigkeit;
- Gesundheitsdaten; und
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Anlage 2 – Technische und Organisatorische Maßnahmen (TOMs)

1 SICHERHEIT.

1.1 Sicherheitsmaßnahmen. Staffbase wird die in dieser Anlage beschriebenen Sicherheitsmaßnahmen aufrechterhalten und kann zusätzliche oder alternative Sicherheitsmaßnahmen durchführen, wobei sichergestellt wird, dass das Sicherheitsniveau der definierten Maßnahmen nicht verringert wird.

1.2 ISO 27001. Staffbase wird ihre ISO/IEC 27001:2013-Zertifizierung (oder einen gleichwertigen Ersatz) aufrechterhalten. Kunden können eine Kopie der aktuellsten ISO-Zertifikate von Staffbase unter https://staffbase.com/de/sicherheit/ (URL: https://www.google.com/url?q=https://staffbase.com/de/sicherheit/&sa=D&ust=1593186574444000) herunterladen.

1.3 Spezifische Sicherheitsmaßnahmen für Mitarbeiter E-Mail: SOC 2. Wenn der Kunde Mitarbeiter E-Mail erworben hat, dann gilt der SOC 2-Bericht von Staffbase (oder ein gleichwertiger Ersatz) für die Nutzung von Mitarbeiter E-

Mail durch den Kunden. Der Kunde kann eine Kopie des aktuellsten SOC-2-Berichts von Staffbase anfordern.

1.4 Spezifische Sicherheitsmaßnahmen für Communications Control: Der Kunde stimmt zu und erkennt an, dass die Staffbase-Zertifizierung nach ISO/IEC 27001:2013 (noch) nicht auf den Staffbase-Dienst “Communications Control” anwendbar ist.

2 ZUTRITTSKONTROLLEN.

2.1 Physische Zutrittskontrolle. Staffbase wird angemessene Maßnahmen ergreifen, um Unbefugte daran zu hindern, physischen Zugang zu Personenbezogenen Daten zu erhalten. Die Sicherheitsmaßnahmen umfassen u.a.:

(a) Die Anwendung wird in ISO 27001-zertifizierten Datenzentren gehostet. Der physische Zugang zu diesen Datenzentren ist stark eingeschränkt.

(b) Die Büros von Staffbase sind gesichert und der Zugang zu den Büros von Staffbase ist auf Mitarbeiter von Staffbase sowie autorisierte Reinigungsdienste beschränkt. Mitarbeiter und Reinigungsdienste erhalten Zugangsmedien (wie Schlüssel und Key Card). Gäste werden an der Tür begrüßt und zur Kontaktperson begleitet. Die Ausgabe und Rückgabe der Zugangsmedien wird schriftlich dokumentiert.

2.2 Interne Zugriffskontrolle. Staffbase wird angemessene Maßnahmen ergreifen, um zu verhindern, dass unbefugte Mitarbeiter von Staffbase Zugriff auf Personenbezogene Daten erhalten. Zu den Sicherheitsmaßnahmen gehören u.a.:

(a) Zugriff auf Personenbezogene Daten des Kunden haben ausgewählte Mitarbeiter von Staffbase in folgenden Rollen:

3rd Level Access – Systemadministrator: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der zugehörigen Kundeninstanz inkl. Datenbank.

2nd Level Access – Supportadmininistration: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der zugehörigen Kundeninstanz, aber keinen Server/Datenbankzugriff.

1st LevelAccess – Customer Success Access: Zugriff auf alle Personenbezogenen 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.

(b) Die oben definierten Rollen werden ausschließlich an den minimal notwendigen Kreis von Staffbase Mitarbeitern vergeben. Die Vergabe der Rollen wird protokolliert und mindestens einmal jährlich überprüft.

2.3 Spezifisch für Mitarbeiter E-Mail: Interne Zugriffskontrolle. Wenn der Kunde Mitarbeiter E-Mail erworben hat, ergreift Staffbase angemessene Maßnahmen, um zu verhindern, dass unbefugtes Staffbase-Personal Zugriff auf Personenbezogene Daten erhalten, die im Zusammenhang mit Mitarbeiter E-Mail verarbeitet werden. Die Internen Zugriffskontrollen in Bezug auf Mitarbeiter E-Mail umfassen unter anderem Folgendes:

(a) Eine ausgewählte Anzahl von Staffbase-Mitarbeitern hat in den folgenden Rollen Zugriff auf Personenbezogene Daten:

Zugriff für Entwickler: Persönlicher Zugriff auf alle Personenbezogenen Daten innerhalb der entsprechenden Kundeninstanz, einschließlich der Datenbank.

Zugriff für Customer Success: Persönlicher Zugriff auf die Kundeninstanz im Namen des jeweiligen Admin-Nutzers, aber kein Server- oder Datenbankzugriff.

(b) Die oben definierten Rollen werden ausschließlich an den minimal notwendigen Kreis von Staffbase-Mitarbeitern vergeben. Die Vergabe der Rollen wird protokolliert und mindestens einmal jährlich überprüft.

2.4 Communications Control spezifische Interne Zugriffskontrolle: Wenn der Kunde Communications Control Dienste erworben hat, wird Staffbase angemessene Maßnahmen ergreifen, um zu verhindern, dass unbefugte Mitarbeiter von Staffbase Zugriff auf Personenbezogene Daten erhalten. Zu den Sicherheitsmaßnahmen gehören u.a.:

(a) Zugriff auf Personenbezogene Daten des Kunden haben ausgewählte Mitarbeiter von Staffbase in folgenden Rollen:

3rd Level Access – Systemadministrator: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der zugehörigen Kundeninstanz inkl. Datenbank.

2nd Level Access – Supportadmininistration: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der zugehörigen Kundeninstanz, und beschränkter Server/Datenbankzugriff.

1st Level Access – ***Customer Success Access:*** Zugriff auf alle Personenbezogenen Daten innerhalb einer Kundeninstanz über die Applikation entsprechend der Freigabe durch den Kunden. 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.

(b) Die oben definierten Rollen werden ausschließlich an den minimal notwendigen Kreis von Staffbase Mitarbeitern vergeben. Die Vergabe der Rollen wird protokolliert und mindestens einmal jährlich überprüft.

2.5 Elektronische Zugangskontrolle. Staffbase ergreift angemessene Maßnahmen, um zu verhindern, dass unbefugte Personen elektronischen Zugriff auf Personenbezogene Daten erhalten. Zu den Sicherheitsmaßnahmen gehören u.a.:

(a) Der Zugang zum Datenverarbeitungssystem ist auf autorisierte Personen beschränkt und erfordert eine Identifizierung und erfolgreiche Authentifizierung durch Benutzername und Passwort unter Verwendung modernster Sicherheitsmaßnahmen.

(b) Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu Datenverarbeitungssystemen sind auf 3rd und 2nd Level Ebene an ein persönliches Credential (Passwort und User ID) geknüpft. Zugänge für temporär beschäftigte Personen (externe Entwickler, Praktikanten, Auszubildende) werden individuell vergeben. Es werden keine wiederverwendbaren Kennungen (z.B. Azubi1) vergeben.

(c) Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist eingerichtet

und wird dokumentiert.

(d) Bei mehr als fünf Minuten Inaktivität der Arbeitsstation bzw. des Terminals wird ein kennwortgeschützter Bildschirmschoner mit Hilfe der betriebssystemeigenen Mechanismen automatisch aktiviert.

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

(f) 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.

(g) Der Zugang zu den Arbeitsstationen sowie zum Passwortmanager wird durch ein Passwort geschützt. Das Passwort muss aus mindestens 10 Zeichen bestehen sowie einem Zeichenmix aus Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben.

2.6 Trennungskontrolle. Die Test- und Staging-Systeme von Staffbase werden logisch von den Produktionssystemen getrennt. Für das Testen ermöglicht Staffbase dedizierte Testdaten.

3 PSEUDONYMISIERUNG & VERSCHLÜSSELUNG.

3.1 Verschlüsselung. Die gesamte Kommunikation unserer Systeme über öffentliche Netze wird nach dem Stand der Technik verschlüsselt. Staffbase verschlüsselt die Benutzerkennwörter mit Hilfe von Best-Practice One-Way-Hash-Functions, und die Kerndatenbanken werden im Ruhezustand mit Verschlüsselungsschemata verschlüsselt, die den besten Praktiken der Branche entsprechen.

3.2 Pseudonymisierung. Staffbase verwendet Pseudonyme zur Speicherung benutzerbezogener Interaktionen, wann immer dies möglich ist.

4 INTEGRITÄT.

4.1 Weitergabekontrolle. Daten werden ausschließlich unter Verwendung des verschlüsselten HTTPS Protokolls ausgetauscht.

4.2 Eingabekontrolle. Die Aktivitäten des Kunden im Zusammenhang mit der Anlage und Aktualisierung von Nutzerdatensätzen werden protokolliert.

5 VERFÜGBARKEIT UND BELASTBARKEIT.

Staffbase hat ein System entwickelt, das dazu dient, Dienstunterbrechungen aufgrund von Naturkatastrophen, Hardware-Ausfällen oder anderen unvorhergesehenen Katastrophen oder Unglücksfällen zu minimieren. Der Disaster Recovery-Ansatz von Staffbase umfasst:

(a) Einsatz hochmoderner Dienstleistungsanbieter, die bei der Erbringung der Dienstleistungen unterstützen.

(b) Backups. Staffbase führt auf allen relevanten Systemen tägliche Backups durch, die bis zu einem Monat gespeichert werden und auf der Grundlage identifizierter Vorfälle zur Wiederherstellung zur Verfügung stehen.

(c) Dual-Mode. Alle Produktionssysteme laufen mindestens im Dual-Mode, um ein schnelles Failover zu ermöglichen.

(d) Weltweite Büros. Staffbase ist weltweit tätig; im Falle regionaler Probleme in einem der Büros von Staffbase können unsere Teams an anderen Standorten Unterstützung leisten, um eine reibungslose Wiederherstellung zu ermöglichen.

(e) Disaster Recovery Plan. Das Disaster Recovery Programm von Staffbase konzentriert sich auf technische Katastrophen für den Betrieb der Staffbase-Plattform und umfasst Pläne für verschiedene Szenarien sowie regelmäßige Schulungen für das Recovery Team. Das Team ist daher in der Lage, in Notfällen Daten wiederherzustellen.

6 PRÜFUNG, BEWERTUNG UND EVALUIERUNG.

6.1 Datenschutz-Management. Staffbase hat für die Verarbeitung von Personenbezogenen Daten Prozesse und Arbeitsabläufe definiert. Die Kontrolle der Umsetzung findet regelmäßig durch das Security-Team und das Legal-Team statt.

6.2 Schulung. Alle Mitarbeiter von Staffbase erhalten jährlich eine Schulung zum Thema Sicherheits- und Datenschutzbewusstsein.

6.3 Kundenanweisungen. Die Personen, die seitens Staffbase befugt sind, Anweisungen des Kunden anzunehmen und auszuführen, werden von Staffbase verbindlich festgelegt. In der Regel sind dies der Account Manager des Kunden sowie Mitarbeiter des Customer Success und Support-Teams von Staffbase.