Staffbase Auftragsverarbeitungsvertrag

1 EINFÜHRUNG

(a) Dieser Auftragsverarbeitungsvertrag ("**AVV**") ist Bestandteil und unterliegt den Bedingungen des Master Subscription Agreement oder einer anderen zwischen Staffbase und dem Kunden geschlossenen Vereinbarung, die die Nutzung der Dienste durch den Kunden regelt (die **"Vereinbarung"**). Jeder in Großbuchstaben geschriebene Begriff, der in diesem AVV verwendet, aber nicht definiert wird, hat die in der Vereinbarung zugeschriebene Bedeutung.

(b) Die Parteien vereinbaren, dass dieser AVV alle bestehenden Auftragsverarbeitungsverträge, die die Parteien zuvor in Verbindung mit den Diensten geschlossen haben, ersetzt.

(c) Der Kunde und Staffbase erkennen an, dass etwaige Haftungsausschlüsse oder -beschränkungen in der Vereinbarung die jeweilige Haftung der Parteien in Bezug auf Ansprüche, die von Betroffenen Personen gemäß den Datenschutzvorschriften erhoben werden, nicht einschränken.

(d) Im Falle eines Widerspruchs zwischen der Vereinbarung und dem AVV hat der AVV Vorrang.

(e) Dieser AVV verwendet die von der Europäischen Kommission hinsichtlich Artikel 28 (3) DSGVO veröffentlichten Standardvertragsklauseln für Auftragsverarbeiter (Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021) (**die „Klauseln**") mit minimalen Abweichungen, um die Prozesse von Staffbase und dessen weltweites Geschäft widerzuspiegeln.

2 DEFINITIONEN

„Datenschutzgesetzen der US-Bundesstaaten" haben die im US State Privacy Law Addendum angegebene Bedeutung.

„Datenschutzvorschriften" bedeutet, soweit anwendbar die Europäische Datenschutzvorschriften

„Drittland" bedeutet **(a)** soweit die DS-GVO auf die Verarbeitung Personenbezogener Daten durch Staffbase Anwendung findet, ein Land außerhalb des EWR, das nicht Gegenstand eines Angemessenheitsbeschlusses der Europäischen Kommission ist; **(b)** soweit die UK Datenschutzvorschriften auf die Verarbeitung Personenbezogener Daten durch Staffbase Anwendung finden, ein Land, das nicht Gegenstand eines Angemessenheitsbeschlusses gemäß Abschnitt 17A des United Kingdom Data Protection Act 2018 ist; und **(c)** soweit das revDSG auf die Verarbeitung Personenbezogener Daten durch Staffbase Anwendung findet, ein Land außerhalb des EWR und/oder der Schweiz, das keinem Angemessenheitsbeschluss des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**„EDÖB"**) unterliegt.

„Eingeschränkte Übermittlung" bedeutet in Fällen, in denen die Europäischen Datenschutzvorschriften Anwendung finden, eine Übermittlung von Personenbezogenen Daten in ein Drittland.

„Europäische Datenschutzvorschriften" bedeutet: **(i)** die Datenschutzgrundverordnung ((EU) 2016/679) (**„DS-GVO"**); **(ii)** die geltenden nationalen Umsetzungen der DS-GVO in der Europäischen Union (**„EU"**) und den Mitgliedstaaten des Europäischen Wirtschaftsraums (**„EWR"**); **(iii)** in Bezug auf das Vereinigte Königreich (**„UK"**), der Data Protection Act 2018 und die DS-GVO, wie sie durch Abschnitt 3 des European Union (Withdrawal) Act 2018 des Vereinigten Königreichs in das Recht des Vereinigten Königreichs übernommen wurden (**„UK Datenschutzvorschriften"**); **(iv)** die ePrivacy-Richtlinie 2002/58/EC der EU in der durch die Richtlinie 2009/136/EG geänderten Fassung; und **(v)** Schweizer Bundesgesetz über den Datenschutz vom 25 September 2020 und seine Ausführungsbestimmungen in ihrer jeweils geänderten, aufgehobenen oder ersetzten Fassung **„(revDSG"**).

„Modellklauseln" bezeichnet, sofern europäische Datenschutzgesetze gelten, die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, die durch den Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 (derzeit hier https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915 einsehbar) erlassen wurde, in der jeweils gültigen Fassung.

„Personenbezogene Daten" sind solche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wenn (i) diese Informationen in Kundeninhalten enthalten sind und (ii) nach geltendem Datenschutzrecht in ähnlicher Weise wie personenbezogene Daten, persönliche Informationen oder personenbezogene identifizierbare Informationen geschützt sind**.**

„UK Anhang" bezeichnet den vom Information Commissioner's Office gemäß § 199 (A) des UK Data Protection Act 2018 herausgegebenen Anhang zum internationalen Datentransfer (derzeit zu finden unter https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), der von Zeit zu Zeit geändert oder ersetzt werden kann.

„Unterauftragsverarbeiter" bezeichnet jeden von Staffbase oder seinen Verbundenen Unternehmen beauftragten Auftragsverarbeiter, der Staffbase bei der Erfüllung seiner Verpflichtungen im Rahmen der Vereinbarung unterstützt. Zu den Unterauftragsverarbeitern können Dritte oder mit Staffbase Verbundene Unternehmen gehören.

"US State Privacy Law Addendum" bezeichnet, sofern Staffbase Personenbezogene Daten, die den Datenschutzgesetzen der US-Bundesstaaten unterliegen als Auftragnehmer für den Kunden verarbeitet den Anhang bzgl. US-amerikanischer staatliche Datenschutzgesetze, der unter https://staffbase.com/en/legal/ zu finden ist.

„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 Zugriff auf Personenbezogene

Daten geführt hat, die von Staffbase und/oder seinen Unterauftragsverarbeitern in Verbindung mit der Erbringung der Dienste übermittelt, gespeichert oder anderweitig verarbeitet werden.

Die Begriffe **„Verantwortlicher“**, **„Betroffene Person“**, **„Auftragsverarbeiter“** und **„Verarbeitung“** haben die Bedeutung, die ihnen nach den Datenschutzvorschriften zukommt, und **„verarbeiten“** und **„verarbeitet“** sind entsprechend auszulegen.

3 DIE KLAUSELN

Klausel 1 - Zweck und Anwendungsbereich

(a) Der Zweck dieses AVV ist es, die Einhaltung der Datenschutzvorschriften in ihrer jeweils gültigen Fassung zu gewährleisten, die von Zeit zu Zeit geändert, ersetzt oder ergänzt werden können.

(b) Staffbase und der Kunde haben diesem AVV zugestimmt, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.

(c) Dieses AVV gilt für die Verarbeitung der in Anhang II beschriebenen Personenbezogener Daten.

(d) Die Anhänge sind ein integraler Bestandteil dieses AVV.

(e) Dieser AVV lässt die Verpflichtungen unberührt, denen der Kunde aufgrund der Datenschutzvorschriften unterliegt.

(f) Dieser AVV allein gewährleistet nicht die Einhaltung der Verpflichtungen im Zusammenhang mit internationalen Übermittlungen in Übereinstimmung mit den Datenschutzvorschriften, sofern diese anwendbar sind.

Klausel 2 – Unabänderbarkeit der Klauseln *[Nicht anwendbar]*

Klausel 3 - Auslegung

(a) Werden in diesem AVV Begriffe verwendet, die in den Datenschutzvorschriften definiert sind, so haben diese Begriffe die gleiche Bedeutung wie in den anwendbaren Datenschutzvorschriften.

(b) Dieser AVV ist im Lichte der Bestimmungen der Datenschutzvorschriften zu lesen und auszulegen, soweit diese anwendbar sind.

(c) Dieser AVV darf nicht in einer Weise ausgelegt werden, die den in den Datenschutzvorschriften vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der Betroffenen Personen beeinträchtigt.

Klausel 4 - Vorrang

Im Falle eines Widerspruchs zwischen diesem AVV und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später geschlossen werden, hat dieser AVV Vorrang.

Klausel 5 - Kopplungsklausel *[Nicht anwendbar]*

Klausel 6 - Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien Personenbezogener Daten und die Zwecke, für die die Personenbezogenen Daten im Auftrag des Kunden verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 - Pflichten der Parteien

7.1 Weisungen

(a) Staffbase verarbeitet Personenbezogene Daten nur auf dokumentierte Weisung des Kunden, es sei denn, Staffbase ist aufgrund lokaler Gesetze, denen Staffbase unterliegt, wie z. B. dem Recht der EU oder eines EU-Mitgliedstaats, dazu verpflichtet. In diesem Fall informiert Staffbase den Kunden vor der Verarbeitung über diese gesetzliche Anforderung, es sei denn, das Gesetz verbietet dies. Die Vereinbarung (einschließlich dieser DPA), alle anwendbaren Bestellformulare und die Nutzung der Dienste stellen die vollständigen Weisungen des Kunden an Staffbase für die Verarbeitung Personenbezogener Daten dar. Der Kunde kann während der gesamten Dauer der Verarbeitung Personenbezogener Daten auch nachträgliche Weisungen erteilen, solange diese mit den Bestimmungen dieser DSGVO und der Vereinbarung übereinstimmen. Diese Weisungen sind stets zu dokumentieren.

(b) Staffbase informiert den Kunden unverzüglich, wenn nach Ansicht von Staffbase die vom Kunden erteilten Anweisungen gegen Datenschutzvorschriften verstoßen.

7.2 Zweckbindung

Staffbase verarbeitet die Personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Kunden erhält.

7.3 Dauer der Verarbeitung Personenbezogener Daten

Die Daten werden von Staffbase nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

(a) Staffbase ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der Personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung des Schutzes Personenbezogener Daten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den

Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die Betroffenen Personen verbundenen Risiken gebührend Rechnung.

(b) Staffbase gewährt seinem Personal nur insoweit Zugang zu den Personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung der Vereinbarung unbedingt erforderlich ist. Staffbase gewährleistet, dass sich die zur Verarbeitung der erhaltenen Personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung Personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten („Sensible Daten"), wendet Staffbase spezielle Beschränkungen und/oder zusätzlichen Garantien an, soweit dies möglich und nach den geltenden Datenschutzvorschriften vorgeschrieben ist. Der Kunde kontrolliert, ob er Sensible Daten in Verbindung mit den Staffbase Diensten verarbeitet, und der Kunde muss die Einhaltung der Datenschutzvorschriften bei der Verarbeitung Sensibler Daten sicherstellen.

7.6 Dokumentation und Einhaltung dieses AVV

(a) Die Parteien müssen die Einhaltung dieses AVV nachweisen können.

(b) Staffbase bearbeitet umgehend Anfragen des Kunden bezüglich der Verarbeitung von Personenbezogenen Daten gemäß diesem AVV umgehend und in angemessener Weise.

(c) Staffbase stellt dem Kunden alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem AVV festgelegten und sich unmittelbar aus den Datenschutzvorschriften ergebenden Pflichten erforderlich sind. Auf Verlangen des Kunden gestattet Staffbase ebenfalls die Prüfung der unter diesen AVV fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Kunde einschlägige Zertifizierungen von Staffbase berücksichtigen.

(d) Der Kunde kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen von Staffbase umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

(e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

(a) Staffbase besitzt die allgemeine Genehmigung des Kunden für die Beauftragung von Unterauftragsverarbeitern, die unter https://staffbase.com/de/legal/unterauftragsverarbeiter/ aufgeführt sind. Staffbase informiert den Kunden mindestens 30 Tage im Voraus ausdrücklich schriftlich über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Kunden damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Staffbase stellt dem Kunden die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt Staffbase einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Kunden), so muss diese Beauftragung im Wege eines Vertrages erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für Staffbase gemäß diesem AVV gelten. Staffbase stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen Staffbase gemäß diesem AVV und den anwendbaren Datenschutzvorschriften unterliegt.

(c) Staffbase stellt dem Kunden auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich Personenbezogener Daten notwendig ist, kann Staffbase den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Staffbase haftet gegenüber dem Kunden in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit Staffbase geschlossenen Vertrag nachkommt. Staffbase benachrichtigt den Kunden, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten in wesentlicher Weise nicht erfüllt.

(e) *[Klausel 7.7 (e) wurde absichtlich gelöscht]*

7.8 Internationale Datenübermittlungen

(a) Jede Übermittlung von Personenbezogenen Daten durch Staffbase an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Kunden oder zur Einhaltung einer speziellen Bestimmung nach dem lokalen Recht, dem Staffbase unterliegt, und in Übereinstimmung mit dem Datenschutzvorschriften (soweit anwendbar). Staffbase kann Personenbezogene Daten an seine Verbundenen Unternehmen oder seine Unterauftragsverarbeiter in einem Drittland übermitteln, vorbehaltlich der Anforderungen an eine Benachrichtigung gemäß Klausel 7.7.

(b) Der Kunde erklärt sich damit einverstanden, dass in Fällen, in denen Staffbase einen Unterauftragsverarbeiter gemäß Klausel 7.7. für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Kunden) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine direkte oder indirekte Übermittlung Personenbezogener Daten in ein Drittland beinhalten, Staffbase und der Unterauftragsverarbeiter die Einhaltung der Europäischen Datenschutzvorschriften sicherstellen können, indem sie die Modellklauseln und gegebenenfalls den UK Anhang verwenden, sofern die Voraussetzungen für die Anwendung dieser Modellklauseln erfüllt sind.

(c) Sofern die Übermittlung Personenbezogener Daten vom Kunden an Staffbase als Eingeschränkte Übermittlung eingestuft wird und die Europäischen Datenschutzvorschriften das Vorhalten angemessener Garantien vorschreiben, unterliegt die Übermittlung den Modellklauseln, die gemäß Anhang V (Modellklauseln) als in diesen AVV aufgenommen gelten und als deren wesentlicher Bestandteil betrachtet werden.

Klausel 8 - Unterstützung des Kunden

(a) Staffbase unterrichtet den Kunden unverzüglich über jeden Antrag, den er von der Betroffenen Person erhalten hat ("**Betroffenenantrag**"). Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Kunden dazu ermächtigt.

(b) Unter Berücksichtigung der Art der Verarbeitung unterstützt Staffbase den Kunden bei der Erfüllung von dessen Pflicht, Anträge Betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben (a) und (b) befolgt Staffbase die Weisungen des Kunden.

(c) Abgesehen von der Pflicht von Staffbase, den Kunden gemäß Klausel 8 Buchstabe (b) zu unterstützen, unterstützt Staffbase unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Kunden zudem bei der Einhaltung der folgenden Pflichten:

(1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz Personenbezogener Daten (eine "Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

(2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Kunde keine Maßnahmen zur Eindämmung des Risikos trifft;

(3) Pflicht zur Gewährleistung, dass die Personenbezogenen Daten sachlich richtig und auf dem neusten Stand sind, indem Staffbase den Kunden unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten Personenbezogenen Daten unrichtig oder veraltet sind

(4) Pflichten aus den Datenschutzvorschriften.

(d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Kunden durch Staffbase bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzungen des Schutzes Personenbezogener Daten

Im Falle einer Verletzung des Schutzes Personenbezogener Daten arbeitet Staffbase mit dem Kunden zusammen und unterstützt ihn entsprechend, damit der Kunde seinen Verpflichtungen gemäß den Datenschutzvorschriften nachkommen kann, wobei Staffbase die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Kunden verarbeiteten Daten

Im Falle einer Verletzung des Schutzes Personenbezogener Daten im Zusammenhang mit den vom Kunden verarbeiteten Daten unterstützt Staffbase den Kunden wie folgt:

(a) bei der unverzüglichen Meldung der Verletzung des Schutzes Personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Kunden die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes Personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

(b) bei der Einholung der folgenden Informationen, die gemäß den Datenschutzvorschriften in der Meldung des Kunden anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

(1) die Art der Personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der Betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen Sätze Personenbezogener Daten;

(2) die wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten;

(3) die vom Kunden ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

(c) bei der Einhaltung der Pflicht gemäß den Datenschutzvorschriften, die betroffene Person unverzüglich von der Verletzung des Schutzes Personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der von Staffbase verarbeiteten Daten

Im Falle einer Verletzung des Schutzes Personenbezogener Daten im Zusammenhang mit den von Staffbase verarbeiteten Daten meldet Staffbase diese dem Kunden unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

(a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der Betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

(b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes Personenbezogener Daten eingeholt werden können;

(c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt. Staffbase ergreift ferner geeignete und angemessene Maßnahmen zur Eindämmung, Untersuchung und Abmilderung einer Verletzung des Schutzes Personenbezogener Daten.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die Staffbase zur Verfügung zu stellen hat, um den Kunden bei der Erfüllung von dessen Pflichten gemäß den Datenschutzvorschriften zu unterstützen.

Klausel 10 – Verstöße gegen diesen AVV und Beendigung der Vereinbarung

(a) Falls Staffbase seinen Pflichten gemäß diesem AVV nicht nachkommt, kann der Kunde – unbeschadet der Bestimmungen der Datenschutzvorschriften – Staffbase anweisen, die Verarbeitung Personenbezogener Daten auszusetzen, bis er diesen AVV einhält oder die Vereinbarung beendet ist. Staffbase unterrichtet den Kunden unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diesen AVV einzuhalten.

(b) Der Kunde ist berechtigt, die Vereinbarung zu kündigen, soweit es die Verarbeitung Personenbezogener Daten gemäß diesem AVV betrifft, wenn

  (1) der Kunde die Verarbeitung Personenbezogener Daten durch Staffbase gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieses AVV nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

  (2) Staffbase in erheblichem Umfang oder fortdauernd gegen diesen AVV verstößt oder seine Verpflichtungen gemäß den anwendbaren Datenschutzvorschriften nicht erfüllt;

  (3) Staffbase einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesem AVV oder anwendbaren Datenschutzvorschriften zum Gegenstand hat, nicht nachkommt.

(c) Staffbase ist berechtigt, die Vereinbarung zu kündigen, soweit es die Verarbeitung Personenbezogener Daten gemäß diesem AVV betrifft, wenn der Kunde auf der Erfüllung seiner Anweisungen besteht, nachdem er von Staffbase darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

(d) Nach Beendigung der Vereinbarung löscht Staffbase nach Wahl des Kunden alle im Auftrag des Kunden verarbeiteten Personenbezogenen Daten und bescheinigt dem Kunden, dass dies erfolgt ist, oder er gibt alle Personenbezogenen Daten an den Kunden zurück und löscht bestehende Kopien, sofern nicht nach den Datenschutzvorschriften eine Verpflichtung zur Speicherung der Personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Staffbase weiterhin die Einhaltung dieses AVV.

ANHANG I:

LISTE DER PARTEIEN

Kunde

Name: Der Kunde, wie in der jeweiligen Bestellung bezeichnet.

Anschrift: Die Adresse des Kunden wie in der jeweiligen Bestellung angegeben.

Name, Funktion und Kontaktdaten der Kontaktperson: Die Kontaktangaben des Kunden wie in der jeweiligen Bestellung oder der Vereinbarung angegeben (soweit einschlägig).

Unterschrift und Beitrittsdatum: Die Unterschrift und das Datum des Kunden wie aus der jeweiligen Bestellung ersichtlich.

Staffbase:

Name: Das Staffbase Unternehmen, wie in der jeweiligen Bestellung bezeichnet.

Anschrift: Die Adresse von Staffbase, wie in der jeweiligen Bestellung angegeben.

Name, Funktion und Kontaktdaten der Kontaktperson: privacy@Staffbase.com.

Unterschrift und Beitrittsdatum: Die Unterschrift und das Datum von Staffbase wie aus der jeweiligen Bestellung ersichtlich.

ANHANG II

BESCHREIBUNG DER VERARBEITUNG

Kategorien von Betroffenen Personen, deren Personenbezogene Daten verarbeitet werden

- Mitarbeiter oder andere Personen, die vom Kunden autorisiert sind, die Dienste zu nutzen oder Zugang zu ihnen zu erhalten;
- In Bezug auf die Produkte Mitarbeiter E-Mail und Staffbase Email: E-Mail-Empfänger;
- In Bezug auf das Produkt Communications Control: Social Media Kontakte.

Kategorien von verarbeiteten Personenbezogenen Daten

Mitarbeiter-App & Front Door Intranet	● **Profilinformationen:** Benutzerprofilinformationen, wie Name, E-Mail-Adresse, Position, Abteilung und Standort sowie weitere erforderliche oder freiwillige Profilinformationen. ● **Anmeldedaten:** E-Mail-Adresse und Passwort. ● **Inhalte:** Alle anderen Personenbezogenen Daten, die in Kundeninhalten enthalten sind, zum Beispiel Personenbezogene Daten in Chats oder in Mediendateien. ● **Technische Informationen:** Gerätetyp, IP-Adresse, Benutzer-ID, Betriebssystem, Browsertyp, Benutzeragent, Zeitstempel der Besuche und lokale Speicherung.
Mitarbeiter E-Mail	● **Kontoinformationen:** Vollständiger Name, E-Mail-Adresse und Passwort der Zugelassenen 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 E-Mail-Newsletter-Vorlagen und Entwürfen sowie Betreffzeilen. ● **E-Mail-Metrik-Informationen:** Ungefährer Standort der E-Mail-Empfänger (zur Identifizierung von Zeitzoneneinstellungen und in Bezug auf interne E-Mail-Metriken); Informationen über das E-Mail-Verhalten, 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 Segmentierungsinformationen, die vom Kunden hochgeladen werden, wie z. B. die Berufsbezeichnung, die Abteilung oder der Bürostandort. ● **Technische Informationen:** Gerätetyp, IP-Adresse, Benutzer-ID, Betriebssystem, Browsertyp sowie Besuchs- und Nutzungsinformationen.
Staffbase Email	● **Profilinformationen:** Benutzerprofilinformationen wie Name, E-Mail-Adresse, Position, Abteilung und Standort sowie andere erforderliche oder freiwillige Profilinformationen. ● **Anmeldedaten**: E-Mail-Adresse und Passwort Autorisierter Benutzer. ● **Inhalte**: Alle anderen personenbezogenen Daten, die in Kundeninhalten enthalten sind, z. B. personenbezogene Daten in E-Mail-Inhalten oder in Mediendateien. ● **E-Mail-Metrik-Informationen**: Informationen über die E-Mail-Interaktion, einschließlich, aber nicht beschränkt auf, wann ein E-Mail-Newsletter gelesen wird, wann ein Link in einem E-Mail-Newsletter angeklickt wird, erfasst durch Tracking-Technologien wie Pixel und personalisierte Links. ● **Technische Informationen**: Gerätetyp, IP-Adresse, Benutzer-ID, Betriebssystem, Browsertyp, Benutzeragent, Zeitstempel der Besuche und lokale Speicherung
Communications Control	● **Kontoinformationen:** Vollständiger Name, E-Mail-Adresse und Passwort der Zugelassenen Nutzer. ● **Social Media Unterhaltungen:** @Handle des Social Media Accounts, Vor- und Nachname der Social Media Kontakte, Inhalte der Nachricht und Unterhaltungsverlauf. ● **Inhalte:** Alle anderen Personenbezogenen Daten, die in Kundeninhalten enthalten sind. ● **Technische Informationen:** Gerätetyp, IP-Adresse, Nutzer-ID, Betriebssystem, Browsertyp, Nutzer-Agent, Zeitstempel der Besuche und lokaler Speicherung.

Besondere Kategorien Personenbezogener Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen des Zugangs zu den Daten, Beschränkungen für die Weitergabe oder zusätzliche Sicherheitsmaßnahmen.

Der Umfang der besonderen Kategorien Personenbezogener Daten wird vom Kunden bestimmt und kontrolliert und kann die folgenden Kategorien betreffen:

- rassische oder ethnische Herkunft;
- politische Meinungen;
- religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftszugehörigkeit;
- Daten über die Gesundheit; und
- Daten über das Sexualleben oder die sexuelle Ausrichtung einer natürlichen Person.

Art der Verarbeitung

Staffbase verarbeitet Personenbezogene Daten in dem Umfang, der für die Bereitstellung, Wartung, Unterstützung und Verbesserung der Dienste erforderlich ist.

Zweck(e), für den/die die Personenbezogenen Daten im Namen des Kunden verarbeitet werden

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

Dauer der Verarbeitung

Staffbase verarbeitet Personenbezogene Daten während der Abonnementdauer und für 30 Tage danach. Anschließend werden die Personenbezogenen Daten gelöscht, sofern nicht schriftlich etwas anderes vereinbart wurde.

Für die Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben

Die Unterauftragsverarbeiter von Staffbase verarbeiten Personenbezogene Daten, soweit dies zur Erbringung der Dienste erforderlich ist. Vorbehaltlich Klausel 7.7. des AVV verarbeiten die Unterauftragsverarbeiter Personenbezogene Daten während der Abonnementdauer und für 30 Tage danach. Anschließend werden die Personenbezogenen Daten gelöscht, sofern nicht schriftlich etwas anderes vereinbart wurde.

ANHANG III

SICHERHEITSMASSNAHMEN

1 SICHERHEITSZERTIFIKATE

***ISO 27001*:** Das Information Security Management System (ISMS) von Staffbase ist ISO/IEC 27001:2013 (oder einen vergleichbaren Ersatz) zertifiziert. Der Kunde kann eine Kopie der aktuellen ISO-Zertifikate von Staffbase unter https://staffbase.com/de/sicherheit/ herunterladen.

System and Organization Controls (SOC) 2 Report („SOC 2"): Das ISMS von Staffbase ist SOC 2-zertifiziert. Vorbehaltlich bestehender Vertraulichkeitsvereinbarungen stellt Staffbase dem Kunden auf Anfrage eine Kopie des aktuellen SOC 2 Type 2-Berichts oder eines Berichts oder einer anderen Dokumentation zur Verfügung, in dem/der die von Staffbase implementierten Kontrollen beschrieben werden, die den SOC 2-Bericht ersetzen oder im Wesentlichen gleichwertig sind.

2 ZUTRITTSKONTROLLEN

Physische Zutrittskontrolle: Staffbase ergreift angemessene Maßnahmen, um zu verhindern, dass unbefugte Personen physischen Zugang zu Personenbezogenen Daten erhalten. Die Sicherheitsmaßnahmen umfassen unter anderem:

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

(b) Der Zugang zu den Büros von Staffbase ist auf Staffbase-Mitarbeiter und autorisierte Personen beschränkt. Gäste werden an der Tür empfangen und zur Kontaktperson begleitet. Die Aus- und Rückgabe der Zugangsmedien wird schriftlich dokumentiert.

(c) Der Zugang zu den Staffbase-Büros wird bei einer Änderung der Aufgaben oder des Status rechtzeitig aufgehoben.

Speziell für Mitarbeiter-App / Haustür-Intranet / Staffbase Email: Interne Zugangskontrolle: Staffbase ergreift angemessene Maßnahmen, um zu verhindern, dass unbefugte Staffbase-Mitarbeiter Zugang zu Kundendaten erhalten. Die Sicherheitsmaßnahmen umfassen unter anderem:

(a) Eine ausgewählte Anzahl von Staffbase-Mitarbeitern hat in den folgenden Rollen Zugang zu Personenbezogenen Daten:

3rd Level Access – Systemadministrator: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der entsprechenden Kundeninstanz, einschließlich der Datenbank.

2nd Level Access – Supportadministration: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der entsprechenden Kundeninstanz, jedoch kein Server- oder Datenbankzugriff.

1st Level Access – Customer Success Access: Zugriff auf alle Personenbezogenen Daten innerhalb einer Kundeninstanz über die Anwendung entsprechend der Freigabe durch den Kunden. Es ist kein Zugriff auf Datenbanken möglich. Zugang zu Customer Support ist nicht personengebunden und steht allen Mitarbeitern des Customer Success/Support Teams von Staffbase zur Verfügung.

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

Speziell für Mitarbeiter E-Mail: Interne Zugriffskontrolle. Wenn der Kunde Mitarbeiter E-Mail bestellt hat, ergreift Staffbase angemessene Maßnahmen, um zu verhindern, dass unbefugte Mitarbeiter von Staffbase Zugang zu Personenbezogenen Daten erhalten, die im Zusammenhang mit Mitarbeiter E-Mail verarbeitet werden. Die Sicherheitsmaßnahmen in Bezug auf Mitarbeiter E-Mail umfassen unter anderem:

(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 an den minimal notwendigen Kreis von Staffbase Mitarbeitern vergeben. Die Vergabe der Rollen wird protokolliert und mindestens einmal jährlich überprüft.

Speziell für Communications Control: Interne Zugriffskontrolle: Wenn der Kunde Communications Control bestellt hat, ergreift Staffbase angemessene Maßnahmen, um zu verhindern, dass unbefugte Mitarbeiter von Staffbase Zugang zu Personenbezogenen Daten erhalten, die im Zusammenhang mit Communications Control verarbeitet werden. Zu den Sicherheitsmaßnahmen in Bezug auf Communications Control umfassen unter anderem:

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

3rd Level Access – Systemadministrator: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der entsprechenden Kundeninstanz, einschließlich der Datenbank.

2nd Level Access – Supportadministration: Personengebundener Zugriff auf alle Personenbezogenen Daten innerhalb der entsprechenden Kundeninstanz, jedoch kein Server- oder Datenbankzugriff.

1st Level Access – Customer Success Access: Zugriff auf alle Personenbezogenen Daten innerhalb einer Kundeninstanz über die Anwendung entsprechend der Freigabe durch den Kunden. Es ist kein Zugriff auf Datenbanken möglich. Zugang zu Customer Support ist nicht personengebunden und steht allen Mitarbeitern des Customer Success/Support Teams von Staffbase zur Verfügung.

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

3 ELEKTRONISCHE ZUGANGSKONTROLLEN

Staffbase ergreift angemessene Maßnahmen, um zu verhindern, dass unbefugte Personen elektronischen Zugriff auf Personenbezogene Daten erhalten. Die Sicherheitsmaßnahmen umfassen unter anderem:

(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 Zugangserkennungen für den Zugang zu Datenverarbeitungssystemen sind auf 3rd und 2nd Level Ebene an persönliche Zugangsdaten (Passwort und User ID) geknüpft. Zugänge für temporär beschäftigte Personen (externe Entwickler, Praktikanten, Auszubildende) werden individuell vergeben. Es werden keine wiederverwendbaren Kennungen (z. B. Praktikant1 etc.) vergeben.

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

(d) Alle Arbeitsstationen und Terminals werden sowohl bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung geschützt (durch manuelle Aktivierung des kennwortgeschützten Bildschirmschoners oder durch Sperrung des Systems). Interne Schulungen werden durchgeführt, um die regelmäßige Anwendung beider Mechanismen zu unterstützen.

(e) Passwörter werden mittels Passwortmanager verwaltet. Der Zugang zu den Arbeitsstationen sowie zum Passwortmanager wird durch ein Passwort geschützt.

4 TRENNUNGSKONTROLLE

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

5 PSEUDONOMYSIERUNG UND VERSCHLÜSSELUNG

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.

Pseudonymisierung. Staffbase verwendet Pseudonyme für die Speicherung von benutzerbezogenen Interaktionen, wann immer dies möglich ist.

6 INTEGRITÄT

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

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

7 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 täglich Backups durch, die bis zu einem Monat lang 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) Globale Niederlassungen. Staffbase ist weltweit tätig, und im Falle regionaler Probleme in einer der Niederlassungen von Staffbase können unsere Teams an allen Standorten Unterstützung leisten, um eine reibungslose Wiederherstellung zu ermöglichen; und

(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.

8 PRÜFUNG, BEWERTUNG UND EVALUIERUNG

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

Schulung: Alle Mitarbeiter von Staffbase erhalten eine jährliche Schulung zum Thema Sicherheit- und Datenschutzbewusstsein.

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

9 MANAGEMENT VON SICHERHEITSVORFÄLLEN

Alle Mitarbeiter, Auftragnehmer und wichtigen Lieferanten sind verpflichtet, Sicherheitsvorfälle zu melden. Staffbase hat einen Plan, um umgehend und systematisch auf alle Sicherheits- oder Verfügbarkeitsvorfälle zu reagieren. Der Staffbase Incident Response Plan basiert auf Industriestandards und besteht aus vier Stufen, die darauf abzielen, Sicherheitsvorfälle zu verhindern, zu identifizieren und zu beheben.

Unser Incident Response Plan umfasst auch einen Problem-Management-Prozess, der dazu dient, Ursachen zu identifizieren und unbekannte Sicherheitsvorfälle zu beheben. Das gesamte Sicherheitsteam ist darin geschult, gemäß dem etablierten Incident Response Plan zu reagieren. Der Incident Response Plan umfasst auch Verfahren für Verletzungen des Schutzes Personenbezogener Daten, und bei solchen Vorfällen ist die Einbeziehung des Datenschutz- und Legal-Teams erforderlich. Betroffene Kunden werden gemäß dem AVV über Verletzungen des Schutzes Personenbezogener Daten informiert.

Dieser Plan wird im Rahmen der ISO 27001-Zertifizierung von Staffbase regelmäßig überprüft und aktualisiert.

10 VULNERABILITY-MANAGEMENT

Für die Produkte von Staffbase wurde ein Prozess zur Vermeidung von Vulnerability eingerichtet, um sicherzustellen, dass Vulnerabilities rechtzeitig erkannt, bewertet und behoben werden. Staffbase verwendet den Industriestandard CVSS-Score, um den Schweregrad der identifizierten Vulnerabilities zu bewerten.

Staffbase beauftragt einen externen Penetrationstester mit der Durchführung unabhängiger Penetrationstests, die mindestens einmal jährlich durchgeführt werden. Eine Zusammenfassung des letzten Penetrationstests ist auf Anfrage vorbehaltlich des Abschlusses einer Geheimhaltungsvereinbarung erhältlich. Interne Penetrationstests werden ebenfalls regelmäßig durchgeführt, um die SOC-2-Anforderungen zu erfüllen.

Staffbase hat ein privates Bug-Bounty-Programm für kontinuierliche Sicherheitstests durch eine globale Gemeinschaft von ethischen Hackern. Das Bug Bounty Programm hat dazu beigetragen, dass sich stetig unsere Sicherheitskontrollen für die Mitarbeiter App und das Front Door Intranet mit großem Erfolg verbessert. Es ist geplant, das Bug Bounty-Programm auch auf unsere anderen Produkte auszuweiten.

ANHANG IV

LISTE DER UNTERAUFTRAGSVERARBEITER

Eine aktuelle Übersicht der Unterauftragsverarbeiter von Staffbase kann hier abgerufen werden: https://staffbase.com/de/legal/unterauftragsverarbeiter/

ANHANG V

MODELLKLAUSELN FÜR EINGESCHRÄNKTE ÜBERMITTLUNGEN NACH EUROPÄISCHEN DATENSCHUTZVORSCHRIFTEN

1 Anwendbarkeit der Modellklauseln

(a) Europäische Union (DS-GVO). Die Parteien vereinbaren, dass, wenn es sich bei der Übermittlung Personenbezogener Daten vom Kunden (als **„Datenexporteur“**) an Staffbase (als **„Datenimporteur“**) um eine Eingeschränkte Übermittlung handelt und die DS-GVO das Vorhalten angemessener Garantien vorschreibt, eine solche Übermittlung den Modellklauseln unterliegt, die durch Verweis als in diesem AVV aufgenommen gelten und einen Teil des AVV bilden, wie im Folgenden darstellt:

- **(i)** Modul 2 (Controller-to-Processor) findet Anwendung, wenn der Kunde ein Verantwortlicher und Staffbase ein Auftragnehmer für Personenbezogene Daten ist; Modul 3 (Processor-to-Processor) findet Anwendung, wenn sowohl der Kunde als auch Staffbase ein Augftragnehmer für Personenbezogene Daten sind. Für jedes Modul, sofern zutreffend:
- **(ii)** in Klausel 7 gilt die optionale Kopplungsklausel nicht;
- **(iii)** in Klausel 8.9 werden alle Prüfungen durch den Kunden gemäß Klausel 7.6. dieses AVV durchgeführt;
- **(iv)** in Klausel 9 gilt die Option 2. Zur Klarstellung: Staffbase hat die allgemeine Genehmigung des Kunden, Unterauftragsverarbeiter gemäß Klausel 7.7. dieses AVV zu beauftragen;
- **(v)** in Klausel 11(a) findet die optionale Formulierung keine Anwendung;
- **(vi)** in Bezug auf Klausel 12 unterliegen alle Ansprüche, die im Rahmen der Modellklauseln geltend gemacht werden, den in der Vereinbarung festgelegten Bestimmungen und Bedingungen. Es wird klargestellt, dass keine Partei ihre Haftung gegenüber den Betroffenen Personen nach den Modellklauseln beschränken darf;
- **(vii)** in Klausel 17 gilt die Option 1. Die Parteien vereinbaren, dass das anwendbare Recht für Streitigkeiten im Zusammenhang mit den Modellklauseln gemäß dem Abschnitt „Anwendbares Recht / Gerichtsstand“ der Vereinbarung bestimmt wird oder, wenn in diesem Abschnitt kein EU-Mitgliedstaat angegeben ist, die Modellklauseln dem Recht der Republik Irland unterliegen;
- **(viii)** in Klausel 18(b) vereinbaren die Parteien, dass der Gerichtsstand für Streitigkeiten im Zusammenhang mit den Modellklauseln gemäß dem Abschnitt “ Anwendbares Recht / Gerichtsstand” der Vereinbarung festgelegt wird oder, wenn in diesem Abschnitt kein EU-Mitgliedsstaat angegeben ist, der Gerichtsstand Dublin (Republik Irland) ist;
- **(ix)** Anhang I der Modellklauseln gilt als mit den in Anhang I und Anhang II dieses AVV aufgeführten Informationen ausgefüllt; und
- **(x)** Anhang II der Modellklauseln gilt als mit den in Anhang III dieses AVV aufgeführten Informationen ausgefüllt.

(b) UK (UK Datenschutzvorschriften). Die Parteien vereinbaren, dass für den Fall, dass es sich bei der Übermittlung Personenbezogener Daten vom Kunden (als “Datenexporteur”) an Staffbase (als “Datenimporteur”) um eine Eingeschränkte Übermittlung nach den UK Datenschutzvorschriften handelt, die Modellklauseln, wie sie in Klausel 7.8.(c) dieses AVV einbezogen werden, mit den folgenden Änderungen gelten:

- **(i)** die Modellklauseln gelten mit den in den UK Datenschutzvorschriften beschriebenen Änderungen, die durch Verweis als in diesem AVV aufgenommen gelten und einen Teil des AVV bilden;
- **(ii)** die Tabellen 1, 2 und 3 in Teil 1 der UK Datenschutzvorschriften gelten als mit den in Anhang II, Anhang III und Anhang IV dieses AVV aufgeführten Informationen ausgefüllt;
- **(iii)** Tabelle 4 in Teil 1 der UK Datenschutzvorschriften gilt als ausgefüllt durch Auswahl der Variante “keine Partei”; und
- **(iv)** etwaige Widersprüche zwischen den Modellklauseln und den UK Datenschutzvorschriften sind gemäß Abschnitt 10 und Abschnitt 11 der UK Datenschutzvorschriften aufzulösen.

(c) Schweiz (revDSG). Die Parteien vereinbaren, dass für den Fall, dass es sich bei der Übermittlung von Personenbezogenen Daten vom Kunden (als “**Datenexporteur**”) an Staffbase (als “**Datenimporteur”**) um eine Eingeschränkte Übermittlung nach dem revDSG handelt, die Modellklauseln, wie sie in Klausel 7.8(c) dieses AVV einbezogen werden, mit den folgenden Änderungen gelten:

- **(i)** in Klausel 13 ist die zuständige Aufsichtsbehörde der EDÖB;
- **(ii)** Verweise auf “EU”, “Union” und “Mitgliedstaat“ in den Modellklauseln beziehen sich auf die Schweiz;
- **(iii)** der Begriff “Mitgliedstaat” ist nicht so auszulegen, dass Betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte geltend zu machen; und
- **(iv)** Verweise auf die “Datenschutzgrundverordnung“, „Verordnung 2016/679“ und „DS-GVO“ in den Modellklauseln beziehen sich auf das revDSG.

2 Beschreibung der Datenverarbeitung gemäß Anhang I der Modellklauseln

A Liste der Parteien

Datenexporteur	**Datenimporteur**

Name: Der Kunde, wie in der Bestellung definiert	Name: Das Staffbase Unternehmen, wie in der Bestellung definiert
Anschrift: Anschrift des Kunden, wie in der Bestellung angegeben	Anschrift: Anschrift von Staffbase, wie in der Bestellung angegeben
Name, Funktion und Kontaktdaten der Kontaktperson: Die Kontaktdaten des Kunden, wie in der Bestellung angegeben	Name, Funktion und Kontaktdaten der Kontaktperson: privacy@Staffbase.com
Rolle: Verantwortlicher	Rolle: Auftragsverarbeiter
Tätigkeiten, die für die gemäß den Modellklauseln übermittelten Daten von Belang sind: Verarbeitung Personenbezogener Daten im Zusammenhang mit der Nutzung der Dienste durch den Kunden	

B Beschreibung der Datenübermittlung

Kategorien Betroffenen Personen	Siehe Anhang II dieses AVV
Kategorien Personenbezogener Daten	Siehe Anhang II dieses AVV
Sensible Daten (falls zutreffend)	Siehe Anhang II dieses AVV
Häufigkeit der Übermittlung	Fortlaufend, abhängig von der Nutzung der Dienste durch den Kunden.
Art der Verarbeitung	Siehe Anhang II dieses AVV
Zweck(e) der Übermittlung	Siehe Anhang II dieses AVV
Dauer der Verarbeitung	Staffbase verarbeitet Personenbezogene Daten während der Abonnementdauer und für 30 Tage danach. Anschließend werden die Personenbezogenen Daten gelöscht, sofern nicht schriftlich etwas anderes vereinbart wurde.
Datenübermittlung durch Unterauftragsverarbeiter	Die Unterauftragsverarbeiter von Staffbase verarbeiten Personenbezogene Daten, soweit dies zur Erbringung der Dienste erforderlich ist. Vorbehaltlich Klausel 7.7. des AVV verarbeiten die Unterauftragsverarbeiter Personenbezogene Daten während der Abonnementdauer und für 30 Tage danach. Anschließend werden die Personenbezogenen Daten gelöscht, sofern nicht schriftlich etwas anderes vereinbart wurde.

C Zuständige Aufsichtsbehörde

Für die Zwecke der Modellklauseln ist die als zuständig anzusehende Aufsichtsbehörde entweder: (i) die Aufsichtsbehörde, die für die Einhaltung der DS-GVO durch den Kunden zuständig ist (wenn der Kunde in einem EU-Mitgliedstaat niedergelassen ist); (ii) die Aufsichtsbehörde des EU-Mitgliedstaats, in dem der Vertreter des Kunden ansässig ist (wenn der Kunde nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den extraterritorialen Anwendungsbereich der DS-GVO fällt und einen Vertreter benannt hat); oder (iii) die Aufsichtsbehörde des EU-Mitgliedstaats, in dem sich die Betroffenen Personen überwiegend befinden (wenn der Kunde nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den extraterritorialen Anwendungsbereich der DS-GVO fällt, ohne einen Vertreter benennen zu müssen). In Bezug auf Personenbezogene Daten, die den UK Datenschutzvorschriften unterliegen, ist die zuständige Aufsichtsbehörde das UK Information Commissioner‘s Office.

In Bezug auf Personenbezogene Daten, die dem RevDSG unterliegen, ist die zuständige Aufsichtsbehörde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (soweit einschlägig).