Vereinbarung über Auftragsverarbeitung gem. Art. 28 DS-GVO

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Propertybase GmbH, Landwehrstr. 63, 80336 München, Germany

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem zwischen dem Auftraggeber und dem Auftragnehmer abgeschlossenen Master Services Agreement, auf das hier verwiesen wird (das Master Services Agreement wird im Folgenden als „Leistungsvereinbarung“ bezeichnet).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung konkret beschrieben. Ergänzend hierzu halten die Parteien folgendes fest: Zwecke der Verarbeitung sind insbesondere: (i) Die Verarbeitung personenbezogener Daten in Übereinstimmung mit der Leistungsvereinbarung und zur Erbringung der dort festgelegten Leistungen; (ii) die Verarbeitung personenbezogener Daten, die vom Auftraggeber bzw. von den, vom Auftraggeber autorisierten Nutzern veranlasst wird; (iii) die Verarbeitung personenbezogener Daten, die durch sonstige, dokumentierte Anweisungen des Kunden veranlasst wird, z.B. Anweisungen, die per E-Mail gegeben werden.

Der Auftragnehmer stellt dem Auftraggeber ein CRM-System (Propertybase) zur Verfügung. Dieses dient dem Auftraggeber zur Kommunikation, Dateiverwaltung, Dateiablage und zur Dokumentation und Sicherung von Unterlagen im Rahmen seiner Kundenbeziehungen. Der

Auftragnehmer übernimmt das Hosting, die Wartung und den Support der Anwender. Hierbei ist eine Zugriffsmöglichkeit auf personenbezogene Daten der Betroffenen nicht ausgeschlossen.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet zum Teil in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, zum Teil in Drittländern statt. Die Verarbeitung in Drittländern erfolgt im Wesentlichen durch die vom Auftragnehmer beauftragten Unterauftragnehmer (siehe auch Ziffer 6 der vorliegenden Vereinbarung).

Der Auftraggeber stimmt der Verarbeitung in Drittländern zu, soweit es sich hierbei um folgende Verarbeitungen handelt:

- Verarbeitung auf den technischen Systemen und Plattformen des Unterauftragnehmers **salesforce.com, Inc.** und der mit diesem verbundenen Unternehmen, wie in Ziffer 6 (7) Tabelle 1 dieser Vereinbarung aufgeführt. Diesbezüglich werden die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt. Das angemessene Schutzniveau in den USA sowie in sonstigen Drittstaaten

  ☒ ist bezüglich der Verarbeitung in den USA festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO), bzw. durch die Selbst-Zertifizierung des Subunternehmers gemäß EU/US Privacy Shield;

  ☒ wird im Hinblick auf die Verarbeitung in den USA und in anderen Drittländern hergestellt durch verbindliche interne Datenschutzvorschriften – Binding Corporate Rules (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

  ☒ wird im Hinblick auf die Verarbeitung in den USA und in anderen Drittländern hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO)

- Verarbeitung auf den technischen Systemen und Plattformen **weiterer Unterauftragnehmer**, die in Ziffer 6 (7) Tabelle 2 dieser Vereinbarung aufgeführt sind. Diesbezüglich werden die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt. Das angemessene Schutzniveau in den USA sowie in sonstigen Drittstaaten

  ☒ ist bezüglich der Verarbeitung in den USA festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO) und durch die Selbst-Zertifizierung des Subunternehmers gemäß EU/US Privacy Shield.

  ☒ wird im Hinblick auf die Verarbeitung in den USA und in anderen Drittländern hergestellt durch verbindliche interne Datenschutzvorschriften – Binding Corporate Rules (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO).

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten (Vorname, Familienname, Titel, Position, Arbeitgeber, Geburtsdatum)
- Account-Daten
- Registrierungsdaten

- Kommunikationsdaten (z.B. Unternehmen, Telefon, E-Mail, Postanschrift)
- Berechtigungsdaten (Zugangsdaten, Benutzername, Passwort)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Nutzungsdaten
- Log-Dateien
- Daten aus sozialen Netzwerken
- Analysedaten
- Kommunikations-und Verbindungsdaten
- ID-Daten von Devices
- Lokalisierungsdaten
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Bilddaten
- Textdateien
- Ggf. weitere Daten, die vom Auftraggeber in Propertybase verarbeitet werden.

(4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Alle Personen, deren Daten vom Auftraggeber in Propertybase verarbeitet werden.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in **Anlage 1**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom vereinbarten Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Dr. Michael Karger, Martiusstr. 5, 80802 München, Tel. 089/38367880 bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in **Anlage 1**].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers bedarf grundsätzlich entweder der gesonderten Zustimmung des Auftraggebers im Einzelfall oder der allgemeinen Genehmigung (Art. 28 Abs. 2 DS-GVO). Der Auftragnehmer muss in jedem Falle dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen implementierten technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der in der Leistungsvereinbarung vereinbarten Leistung beauftragt. Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn kein Zugriff auf Daten des Auftraggebers erfolgen kann), Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Einbindung von Entsorgungsunternehmen ist jedoch anzeigepflichtig, wenn der Kern der Beauftragung die Entsorgung von Dokumenten/Datenträgern welche Daten des Auftraggebers enthalten, beinhaltet. Der Auftragnehmer wird jedoch auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen und erforderliche Kontrollmaßnahmen ergreifen, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

(3) Bei Beauftragung von Subunternehmern hat der Auftragnehmer vertraglich sicherzustellen, dass die zwischen ihm und dem Auftraggeber vereinbarten Regelungen auch gegenüber Subunternehmern gelten.

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(5) Der Auftraggeber genehmigt allgemein, dass der Auftragnehmer weitere bzw. andere Subunternehmer einbindet. Der Auftragnehmer hat den Auftraggeber aber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Subunternehmers

zu informieren, indem er dies nach seiner Wahl entweder dem benannten Ansprechpartner des Auftraggebers mitteilt oder eine Liste mit allen jeweils eingesetzten, weggefallenen und neu hinzukommenden Subunternehmern veröffentlicht. Der Auftraggeber kann gegen derartige Änderungen innerhalb einer Frist von sieben Tagen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund für den Einspruch vor und die Parteien erzielen keine einvernehmliche Lösung über das weitere Vorgehen, wird sich der Auftragnehmer bemühen, dem Auftraggeber eine Leistungsänderung anzubieten oder diesem eine wirtschaftlich angemessene Änderung der Konfiguration oder der Nutzung der Leistungen zu empfehlen, um eine Verarbeitung personenbezogener Daten durch den abgelehnten Unterauftragnehmer zu vermeiden, ohne hierbei den Auftraggeber unverhältnismäßig zu belasten. Sofern der Auftragnehmer eine entsprechende Änderung nicht innerhalb angemessener Zeit (längstens innerhalb von 30 Tagen) zur Verfügung stellen kann oder der Auftraggeber die angebotene Leistungsänderung ablehnt, ist jede der Parteien berechtigt, die betreffenden Leistungen im Hinblick auf diejenigen Leistungen zu kündigen, die vom Auftragnehmer nicht ohne Einsatz des abgelehnten Unterauftragnehmers erbracht werden können. Die Kündigung bedarf einer schriftlichen Erklärung gegenüber dem Auftragnehmer. Der Auftragnehmer wird dem Auftraggeber in diesem Fall vorausgezahlte Vergütungen für die Restlaufzeit, der des betreffenden Vertrags anteilig im Hinblick auf die abgekündigten Leistungen zurückerstatten.

(6) Für den Auftragnehmer sind bereits bei Abschluss dieses Vertrages die unter Ziffer 6 (7) Tabelle 1 und Tabelle 2 in diesem Vertrag bezeichneten Subunternehmer mit der Verarbeitung von Daten in dem dort genannten Umfang beschäftigt. Zu diesen weist der Auftragnehmer auf Anfrage nach, dass die in dieser Ziffer 6 genannten Voraussetzungen für die Beauftragung dieser Subunternehmer eingehalten worden sind. Der Auftraggeber erklärt sich der Auftraggeber mit der Beauftragung der in den Tabelle 1 und 2 genannten Subunternehmer einverstanden.

(7) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 und Art.44 ff. DS-GVO:

Tabelle 1: Unterauftragnehmer salesforce.com, Inc. und mit dieser verbundene Unternehmen		
Firma Unterauftragnehmer	Anschrift/Land	Leistung
salesforce.com, Inc.	Salesforce.com, Inc., The Landmark @ One Market St., Suite 300 San Francisco, California 94105 USA	Core Data Store of Propertybase Customers, Platform, OEM Services

salesforce.com EMEA Limited	England and Wales	Gegebenenfalls eingebunden in die Leistungen von salesforce.com, Inc.
Kabushi Kaisa Salesforce.com	Japan	Gegebenenfalls eingebunden in die Leistungen von salesforce.com, Inc.
Salesforce.com Singapore Pte Ltd.	Singapore	Gegebenenfalls eingebunden in die Leistungen von salesforce.com, Inc.
Salesforce.com Canada Corporation	Canada	Gegebenenfalls eingebunden in die Leistungen von salesforce.com, Inc.
SFDC Australia Pty Ltd	New South Wales, Australia	Gegebenenfalls eingebunden in die Leistungen von salesforce.com, Inc.
Demandware, LLC	USA	E-Commerce Platform and Online Shop
Krux Digital LLC	USA	Data Management Platform
Heroku, Inc.	USA	Email Processing, PDF Processing, Portal Publishing

Tabelle 2: Weitere Unterauftragnehmer		
Firma Unterauftragnehmer (weitere)	Anschrift/Land	Leistung
Amazon.com, Inc.	Amazon.com, Inc. 2021 Seventh Ave Seattle, Washington 98121 USA	Amazon Web Services, Image Store
Basecamp, LLC	Basecamp, LLC. 30 N. Racine Ave, Suite 200 Chicago, Illinois 60607, USA	Project Management
Bugsnag, Inc.	Bugsnag, Inc. 939 Harrison St, San Francisco, CA 94107, USA	Automated Crash Detection Platform
CampainMonitor	Level 38, 201 Elizabeth Street, Sydney NSW 2000, Australia	Mass Email Service
Digital Ocean, LLC	DigitalOcean, LLC 101 Avenue of the Americas	Image Processing

	New York, New York 10013, USA	
GitHub, Inc.	GitHub, Inc. 88 Colin P Kelly Jr Street San Francisco, California 94107, USA	File Hosting for Software Development
Mailgun	535 Mission St. – 14th Floor San Francisco, CA 94105 USA	Mass Email service
Mandrill	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Mass Email service
Mixpanel, Inc.	Mixpanel, Inc. 405 Howard St., Flr 2, San Francisco, CA 94105, USA	Business Analytics Service
Papertrail	7171 Southwest Parkway Bldg 400 Austin, Texas 78735 USA	Logging Management
Propertybase AUS	167 Macquarie Street, Level 13 NSW, Sydney	Customer Service
Propertybase, Inc.	Propertybase Inc., 2560 28th Street, #202, Boulder, CO 80301, USA	Customer Service
Sendgrid	SendGrid, Inc. 1801 California Street, Suite 500 Denver, Colorado 80202, USA	Email Transmission
Slack Technologies, Inc.	Slack Technologies, Inc. 500 Howard Street San Francisco, California 94105, USA	Online Workplace Productivity Tools and Platform
Tableau Software, Inc.	Tableau Software, Inc.	Visualization of Data, Reporting

	Tableau Software 837 N. 34th St. Ste. 200, Seattle, WA, USA	
Zendesk, Inc.	Zendesk, Inc. 1019 Market Street, 6th Floor San Francisco, California 94103, USA	Help Center, Support
Zoom.us	San Jose Office 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113	Screensharing for clients and prospects

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmers erfolgen insbesondere durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsvereinbarung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung

datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Bestimmungen

(1) Die Bestimmungen der Leistungsvereinbarung zur Begrenzung der Haftung des Auftragnehmers finden auch auf diese Vereinbarung Anwendung.

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

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch im elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass sich um eine Änderung oder Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

(4) Bei etwaigen Widersprüchen gehen die Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Leistungsvereinbarung zum Datenschutz vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Teile dieser Vereinbarung nicht.

(5) Auf diese Vereinbarung und alle damit im Zusammenhang stehenden Fragen und Streitigkeiten findet ausschließlich deutsches Recht Anwendung, unter Ausschluss aller Rechtsnormen, die in eine andere Rechtsordnung verweisen.

München, 25.10.2018	…….
DocuSigned by: Max-Michael Mayer 56BAAB58C0160412…	Ort/Datum
Max-Michael Mayer (Geschäftsführer)	Name/Position (in Druckschrift)
DocuSigned by: Michael Wenglein 771D3B47B17D4DD…	…….
Michael Wenglein (Geschäftsführer)	Unterschrift Auftraggeber

Anlage 1 – Technisch-organisatorische Maßnahmen

Salesforce und Heroku: https://help.salesforce.com/articleView?id=Salesforce-Services-Trust-and-Compliance-Documentation&type=1&language=en_US

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Als Auftragsverarbeiter trifft der Auftragnehmer zusätzlich zu Maßnahmen, die sich aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen ergeben oder durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine Maßnahmen zur Pseudonymisierung.
- Verschlüsselung
- sichere Passwortverwaltung in verschlüsseltem Passwortmanager, Verschlüsselung von Datenträgern und Computern, Zugriff ausschließlich über SSL verschlüsselte Verbindungen

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Büros: Schlüssel, elektrische Türöffner, definierter Prozess zur Schlüsselverwaltung
- Zugangskontrolle
  Keine unbefugte Systembenutzung, (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern und Computern, sichere Passwortverwaltung in verschlüsseltem Passwortmanager
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Berechtigungskonzept und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähig, Sandboxing

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Zugriff ausschließlich über SSL verschlüsselte Verbindungen
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Protokollierung und Dokumentenmanagement

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Alle Daten werden ausschließlich in hochverfügbaren Clouddiensten verarbeitet, so dass keine Abhängigkeit des Auftragnehmers von Hardware und Standorten besteht.
- Regelmäßige Prüfung der Systemsicherheit der Clients durch interne Audits per Software und Vorgesetztem.

5. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- Echtzeitreplikation der Daten in der Cloud.
- Dockertechnologie zur schnellsten Wiederherstellbarkeit der Server

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.