1. Präambel

Die Matrix42 Marketplace GmbH, Elbinger Straße 7 in 60487 Frankfurt am Main ("**Auftragnehmer**") stellt

_____
(Vollständige Firma und Adresse des Kunden)

("**Auftraggeber**") gemäß den "Allgemeine Geschäftsbedingungen für Software-as-a-Service (SaaS) - Stand Juli 2014“ ("**AGB SaaS**") sowie der zugehörigen Dienste-Bedingungen (gemeinsam "**Hauptvertrag**") ihre Softwareprodukte ("**Software**") zur Nutzung über das Internet zur Verfügung. Die Software wird von dem Auftragnehmer in einem Rechenzentrum betrieben und dem Auftraggeber zur Nutzung über das Internet zur Verfügung gestellt (auch als "Software as a Service" Modell bezeichnet).

2. Gegenstand

(1) Verarbeitung personenbezogener Daten. Diese Vereinbarung ("**Vertrag**") regelt die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, die (i) der Auftraggeber bzw. deren Benutzer im Rahmen der Verwendung der Software in diese eingibt, (ii) die mit der Nutzung der Software entstehen oder sonst erhoben werden, und (iii) die der Auftraggeber im Zusammenhang mit der Durchführung des Hauptvertrages dem Auftragnehmer in sonstiger Weise überlässt ("**Daten**"). Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Inhalt der Auftragsdatenverarbeitung. Gegenstand der Auftragsdatenverarbeitung ist die Bereitstellung der Software zur Nutzung durch den Auftraggeber im Wege des Zugriffs über das Internet. Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung der Daten ergeben sich aus der Leistungsbeschreibung des Hauptvertrages. Die betroffenen Personenkreise und Datenkategorien sind in den jeweiligen Dienste-Bedingungen genannt.

3. Pflichten des Auftraggebers

(1) Verantwortliche Stelle. Der Auftraggeber bleibt alleinige verantwortliche Stelle der Daten im Sinne des Datenschutzrechts (§ 3 Abs. 7 BDSG) und ist für die Rechtmäßigkeit der Datenverarbeitung, -erhebung und -nutzung sowie für die Wahrung der Rechte der Betroffenen alleine verantwortlich. Dies gilt auch im Hinblick auf die Einhaltung etwaiger besonderer gesetzlicher Schweigepflichten des Auftraggebers (z.B. für Ärzte, Rechts-anwälte und bestimmte Versicherungen, § 203 StGB). Falls erforderlich, hat der Auftraggeber die Betroffenen (z.B. seine Beschäftigten oder Kunden) über Datenverarbeitungen zu informieren oder entsprechende Einwilligungen einzuholen.

(2) Weisungen. Die Datenerhebung, -verarbeitung und -nutzung durch den Auftragnehmer erfolgt im Rahmen der zur Verfügungsstellung einer standardisierten aber konfigurierbaren Software über das Internet. Der Auftraggeber übt sein Weisungsrecht (siehe Ziffer 4.2) in Bezug auf die Daten entsprechend durch Einrichtung und Benutzung der Software aus. Im Übrigen sind Weisungen schriftlich zu erteilen oder mündliche Weisungen unverzüglich schriftlich zu bestätigen. Dem Auftraggeber bleiben Weisungen im Wesentlichen bei gesondert zu vereinbarenden und zu vergütenden Anpassungen der Software oder Datenmigration vorbehalten. Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber gemäß dem Hauptvertrag schuldet, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten. Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht dem Auftragnehmer ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

(3) Pflicht zur Freistellung. Machen Dritte (einschließlich öffentliche Stellen) gegenüber dem Auftragnehmer Ansprüche bzw. Rechtsverletzungen geltend, die auf der Behauptung beruhen, dass der Auftraggeber gegen seine vertraglichen Pflichten verstoßen hat, insbesondere wenn Betroffene gegen den Auftragnehmer mit der Behauptung vorgehen, die Verarbeitung der Daten verstoße gegen ihre Rechte, so gilt Folgendes:

Der Auftraggeber wird den Auftragnehmer von diesen Ansprüchen unverzüglich freistellen, dem Auftragnehmer bei der Rechtsverteidigung angemessene Unterstützung bieten und den Auftragnehmer

von den Kosten der Rechtsverteidigung freistellen. Voraussetzung für diese Freistellungspflicht ist, dass der Auftragnehmer den Auftraggeber über geltend gemachte Ansprüche unverzüglich schriftlich informiert, keine Anerkenntnisse oder gleichkommende Erklärungen abgibt und es dem Auftraggeber ermöglicht, auf Kosten des Auftraggebers - soweit möglich - alle gerichtlichen und außergerichtlichen Verhandlungen über die Ansprüche zu führen.

4. Pflichten des Auftragnehmers

(1) Weisungsgebundenheit. Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen und zum Zwecke der Bereitstellung der Software für den Auftraggeber und nach den Weisungen des Auftraggebers. Der Auftragnehmer verwendet die personenbezogenen Daten für keine anderen Zwecke, gibt die Daten insbesondere nicht unbefugt an Dritte weiter.

(2) Hinweispflicht. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte schriftliche Weisung nach Meinung des Auftragnehmers gegen das BDSG oder gegen andere Vorschriften über den Datenschutz verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht für den Auftragnehmer nicht.

(3) Berichtigung, Löschung und Sperrung. Sind personenbezogene Daten zu berichtigen, löschen oder zu sperren, nimmt dies der Auftraggeber durch Nutzung der entsprechenden Funktionen der Software selbst vor. Ist dies nicht möglich, übernimmt der Auftragnehmer die Berichtigung, Löschung oder Sperrung nach den Weisungen des Auftraggebers. Für die Herausgabe und Löschung der Daten bei Vertragsende gilt Ziffer 9(4) der AGB SaaS.

(4) Ort der Datenverarbeitung. Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt, sofern der Auftraggeber den Auftragnehmer nicht in diesem Vertrag oder in sonstiger Weise eine Verarbeitung in einem Land außerhalb der EU und des EWR gestattet.

(5) Datenschutzbeauftragter. Der Auftragnehmer wird, einen Datenschutzbeauftragten bestellen und auf Anfrage dem Auftraggeber die Kontaktdaten mitteilen.

(6) Datengeheimnis. Der Auftragnehmer wird seine Beschäftigten, die mit der Verarbeitung personenbezogenen Daten betraut sind, mit den maßgebenden Bestimmungen des Datenschutzes vertraut machen und sie schriftlich gemäß § 5 BDSG auf das Datengeheimnis verpflichten.

(7) Meldepflicht. Gelangen Daten, die unter § 42a Ziffer 1 bis 4 BDSG fallen, unrechtmäßig, d.h. unter Verstoß gegen anwendbares Datenschutzrecht, diesen Vertrag oder Weisungen des Auftraggebers, zur Kenntnis eines unbefugten Dritten und drohen dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich.

(8) Unterstützungspflicht. Sofern der Auftraggeber seine Pflicht, einem Betroffenen Auskunft über die Verarbeitung seiner personenbezogenen Daten zu geben, nur mit Hilfe des Auftragnehmers erfüllen kann, wird der Auftragnehmer den Auftraggeber hierbei angemessen unterstützen. Den entstehenden Aufwand hat der Auftraggeber dem Auftragnehmer zu erstatten.

(9) Technische und organisatorische Maßnahmen. Der Auftragnehmer trifft in seinem Verantwortungsbereich angemessene technische und organisatorische Maßnahmen zum Schutz der Daten (§ 9 BDSG und Anlage zu § 9 BDSG) und dokumentiert diese. Die bei Vertragsbeginn getroffenen Maßnahmen sind im Anhang zu diesem Vertrag beschrieben.

5. Kontrollrechte des Auftraggebers

(1) Kontrollen. Der Auftraggeber ist in Bezug auf seine Daten berechtigt, die Einhaltung (i) der gesetzlichen Vorschriften über den Datenschutz, (ii) der vertraglichen Vereinbarungen der Parteien und (iii) der Weisungen des Auftraggebers im erforderlichen Umfang beim Auftragnehmer zu kontrollieren. Kontrollen in den Betriebsstätten des Auftragnehmers muss der Auftraggeber rechtzeitig vorher

schriftlich ankündigen. Kontrollen sind zu den üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs des Auftragnehmers durchzuführen.

(2) Kosten. Durch Kontrollen entstehende Kosten trägt der Auftraggeber, dies umfasst auch eine branchenübliche Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

(3) Schutzwürdige Interessen des Auftragnehmers. Soweit durch Kontrollen Betriebs- und Geschäftsgeheimnisse des Auftragnehmers offenbart oder geistiges Eigentum des Auftragnehmers gefährdet werden kann, hat der Auftraggeber die Kontrollen durch einen fachkundigen und unabhängigen Dritten vornehmen zu lassen, der sich gegenüber dem Auftragnehmer vorab schriftlich zur Verschwiegenheit verpflichtet.

6. Unterauftragsverhältnisse

(1) Gestattung von Unterauftragnehmern. Der Auftragnehmer ist berechtigt, Unterauftrag-nehmer mit Sitz innerhalb der EU oder des EWR einzuschalten. Derzeit nutzt der Auftragnehmer als Hoster die Firmen NTT Europe Ltd. Germany mit Sitz Bleidenstraße 6-10 in 60311 Frankfurt am Main sowie Microsoft Irland Operations Limited mit Sitz in Dublin.

(2) Subunternehmerverträge. Der Auftragnehmer wird mit den Unterauftragnehmern einen Vertrag schließen, der den Anforderungen des § 11 Bundesdatenschutzgesetz genügt.

(3) Auskunftsrecht. Auf Verlangen teilt der Auftragnehmer dem Auftraggeber mit, welche Unter-auftragnehmer der Auftragnehmer zur Datenerhebung, -verarbeitung und/oder -nutzung eingeschaltet hat und welche Dienstleistungen diese für den Auftragnehmer übernehmen.

7. Laufzeit

(1) Laufzeit. Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

(2) Daten bei Vertragsende. Für die Herausgabe und Löschung der Daten bei Vertragsende gilt Ziffer 9(4) der AGB SaaS.

8. Schlussbestimmungen

(1) Anwendbares Recht. Auf diesen Vertrag findet ausschließlich deutsches Recht unter Ausschluss des UN Kaufrechts Anwendung.

(2) Gerichtsstand. Ist der Kunde Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, so ist ausschließlicher Gerichtsstand Hamburg.

Für den **Auftraggeber**	Für den **Auftragnehmer (Matrix42 AG)**
_____	_____
Name (in Blockbuchstaben)	Name (in Blockbuchstaben)
_____	_____
Position / Funktion	Position / Funktion
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift

ANHANG: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

A1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Sicherheitsschlösser
- Chipkartenleser
- Alarmanlage

A2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (einschließlich Verschlüsselungsverfahren):

- Benutzerkennung mit Passwort
- Firewall

A3. Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (einschließlich Verschlüsselungsverfahren):

- Berechtigungskonzept
- Benutzerkennung mit Passwort
- Gesicherte Schnittstellen wie Netzwerk
- Datenträgerverwaltung
- Zertifikatsbasierte Zugriffsberechtigung

A4. Weitergabekontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (einschließlich Verschlüsselungs-verfahren):

- Sicherung bei der elektronischen Übertragung:
- Verschlüsselung
- VPN
- Firewall

A5. Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

- Protokollierung
- Benutzeridentifikation

A6. Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- Weisungsbefugnisse vergeben
- Stichprobenprüfung
- Kontrollrecht
- Datenschutzvertrag nach Vorgaben §11 BDSG

A7. Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):

- Brandschutzmaßnahmen
- Überspannungsschutz
- Unterbrechnungsfreie Stromversorgung
- Klimaanlage
- Festplattenspiegelung
- Backupkonzept
- Virenschutzkonzept

A8. Zweckbindung

Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Trennung von Produktiv- und Testsystemen
- Getrennte Datenbanken