Auftragsdatenverarbeitungsvertrag

Gemäß § 11 Bundesdatenschutzgesetz und (EU) 2016/679 (Datenschutz-Grundverordnung)

Anhang zu den Allgemeinen Geschäftsbedingungen für Software-as-a-Service

1. Präambel

Die hyperspace GmbH, Plaggestr. 24, 264419 Schortens ("hyperspace") stellt

_____

(Vollständige Firma und Adresse des Kunden)

("Kunde") gemäß den "Allgemeine Geschäftsbedingungen für Software-as-a-Service (SaaS) - Stand Juni 2013“ ("AGB SaaS") sowie der zugehörigen Service-Bedingungen (gemeinsam "Hauptvertrag") ihre Softwareprodukte ("Software") zur Nutzung über das Internet zur Verfügung. Die Software wird von hyperspace in einem Rechenzentrum betrieben und dem Kunden 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 Kunde 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 Kunde im Zusammenhang mit der Durchführung des Hauptvertrages hyperspace 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 Kunden 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 Service-Bedingungen genannt.

3. Pflichten des Kunden

(1) Verantwortliche Stelle: Der Kunde 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 Kunden (z.B. für Ärzte, Rechtsanwälte und bestimmte Versicherungen, § 203 StGB). Falls erforderlich, hat der Kunde die Betroffenen (z.B. seine Beschäftigten oder Kunden) über Datenverarbeitungen zu informieren oder entsprechende Einwilligungen einzuholen.

(2) Weisungen: Die Datenerhebung, -verarbeitung und -nutzung durch hyperspace erfolgt im Rahmen der zur Verfügungstellung einer standardisierten, aber konfigurierbaren Software über das Internet. Der Kunde 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 Kunden bleiben Weisungen im Wesentlichen bei gesondert zu vereinbarenden und zu vergütenden Anpassungen der Software oder Datenmigration vorbehalten. Geht der Inhalt von Weisungen des Kunden über dasjenige hinaus, was hyperspace dem Kunden gemäß dem Hauptvertrag schuldet, hat der Kunde die entsprechenden Leistungen hyperspace gesondert zu vergüten. Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht hyperspace ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

(3) Pflicht zur Freistellung: Machen Dritte (einschließlich öffentliche Stellen) gegenüber hyperspace Ansprüche bzw. Rechtsverletzungen geltend, die auf der Behauptung beruhen, dass der Kunde gegen seine vertraglichen Pflichten verstoßen hat, insbesondere wenn Betroffene gegen hyperspace mit der Behauptung vorgehen, die Verarbeitung der Daten verstoße gegen ihre Rechte, so gilt Folgendes: Der Kunde wird hyperspace von diesen Ansprüchen unverzüglich freistellen, hyperspace bei der Rechtsverteidigung angemessene Unterstützung bieten und hyperspace von den Kosten der Rechtsverteidigung freistellen. Voraussetzung für diese Freistellungspflicht ist, dass hyperspace den

Kunden über geltend gemachte Ansprüche unverzüglich schriftlich informiert, keine Anerkenntnisse oder gleichkommende Erklärungen abgibt und es dem Kunden ermöglicht, auf Kosten des Kunden - soweit möglich - alle gerichtlichen und außergerichtlichen Verhandlungen über die Ansprüche zu führen.

4. Pflichten von hyperspace

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

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

(3) Berichtigung, Löschung und Sperrung: Sind personenbezogene Daten zu berichtigen, löschen oder zu sperren, nimmt dies der Kunde durch Nutzung der entsprechenden Funktionen der Software selbst vor. Ist dies nicht möglich, übernimmt hyperspace die Berichtigung, Löschung oder Sperrung nach den Weisungen des Kunden. 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 Kunde hyperspace nicht in diesem Vertrag oder in sonstiger Weise eine Verarbeitung in einem Land außerhalb der EU und des EWR gestattet.

(5) Datenschutzbeauftragter: Als externer Datenschutzbeauftragter für hyperspace gemäß § 4f Absatz 1 Bundesdatenschutzgesetz ist ab dem 01.07.2017 Herrn René Rautenberg, René Rautenberg GmbH, Otto-Hahn-Str. 13b, 85521 Riemerling bestellt.

(6) Datengeheimnis: hyperspace 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 Kunden, zur Kenntnis eines unbefugten Dritten und drohen dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, informiert hyperspace den Kunden hierüber unverzüglich.

(8) Unterstützungspflicht: Sofern der Kunde seine Pflicht, einem Betroffenen Auskunft über die Verarbeitung seiner personenbezogenen Daten zu geben, nur mit Hilfe von hyperspace erfüllen kann, wird hyperspace den Kunden hierbei angemessen unterstützen. Den entstehenden Aufwand hat der Kunde hyperspace zu erstatten.

(9) Technische und organisatorische Maßnahmen: hyperspace 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 Kunden

(1) Kontrollen: Der Kunde 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 Kunden im erforderlichen Umfang bei hyperspace zu kontrollieren. Kontrollen in den Betriebsstätten von hyperspace muss der Kunde rechtzeitig vorher schriftlich ankündigen. Kontrollen sind zu den üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs bei hyperspace durchzuführen.

(2) Kosten: Durch Kontrollen entstehende Kosten trägt der Kunde, dies umfasst auch eine branchenübliche Aufwandsentschädigung für die Arbeitszeit des von hyperspace beanspruchten Personals.

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

6. Unterauftragsverhältnisse

(1) Gestattung von Unterauftragnehmern: hyperspace ist berechtigt, Unterauftragnehmer mit Sitz innerhalb der EU oder des EWR einzuschalten. Derzeit nutzt hyperspace als Hoster die Firma Hostway Deutschland GmbH mit Sitz in Hannover, Deutschland.

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

(3) Auskunftsrecht: Auf Verlangen teilt hyperspace dem Kunden mit, welche Unterauftragnehmer hyperspace zur Datenerhebung, -verarbeitung und/oder -nutzung eingeschaltet hat und welche Dienstleistungen diese für hyperspace 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 Schortens.

9. EU-Datenschutz-Grundverordnung

Ab dem 25.05.2018 ändert sich die gesetzliche Grundlage für die Auftragsdatenverarbeitung (fortan: Auftragsverarbeitung). Mit den nachfolgenden Regelungen wird dieser Vertrag auf die gesetzlichen Anforderungen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, folgend: DSGVO) angepasst und ergänzt. Es ist Wille der Parteien, dass alle Voraussetzungen und Anforderungen an eine rechtskonforme Auftragsverarbeitung nach der DSGVO erfüllt oder geschaffen werden. Abschnitt 9 dieses Vertrages gilt ab dem 25.05.2018.

Der Vertrag dient ab diesem Zeitpunkt der Umsetzung der Anforderungen nach Art. 28 DSGVO. Regelungen, die die vorherige Gesetzeslage referenzieren, finden unter der DSGVO entsprechende Anwendung.

(1) Zu Abschnitt 2,3 dieses Vertrages gilt ergänzend:

Die Datenverarbeitung erfolgt nur auf Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt. Mündliche Weisungen sind anschließend vom Verantwortlichen zu dokumentieren.

(2) Zu Abschnitt 4 dieses Vertrages gilt ergänzend:

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die den Vorgaben des Art. 32 DSGVO entsprechen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten (Art. 32 Abs. 3 lit. c, f DSGVO). Bereits vereinbarte Dokumentationen und IT-Sicherheitskonzepte behalten ihre Wirksamkeit. Der Auftragsverarbeiter wirkt nach Maßgabe des Art. 28 Abs. 3 lit. f DSGVO bei

der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO mit. Er hat dem Verantwortlichen die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

Der Auftragsverarbeiter unterstützt den Verantwortlichen gemäß Art. 28 Abs. 3 lit. e DSGVO nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person nach Kapitel 3 DSGVO erfüllen kann, z.B. die Information und Auskunft an den Betroffen, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch.

Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person binnen 72 Stunden zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragsverarbeiter den Verantwortlichen gemäß Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Verantwortlichen melden und hierbei zumindest folgende Informationen mitteilen:

- eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Für den Kunden:	Für hyperspace GmbH:
_____	_____
Name (in Blockbuchstaben)	Name (in Blockbuchstaben)
_____	_____
Position / Funktion	Position / Funktion
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	Unterschrift

ANHANG: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Hyperspace nutzt als Subunternehmer für den Rechenzentrumsbetrieb die Hostway Deutschland GmbH, Am Mittelfelde 29, 30519 Hannover. Der Betrieb der Server erfolgt in Hannover. Hostway ist durch das Bundesamt für Sicherheit in der Informationstechnik nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert (BSI-IGZ-0230).

Die hier aufgeführten technischen und organisatorischen Maßnahmen beziehen sich auf Hostway in Hannover (H) und hyperspace in Schortens (S).

A1. Zutrittskontrolle

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

- Sicherheitsschlösser (H,S)
- Sicherheitsbeschläge (H,S)
- Elektronische Zutrittskontrollsysteme (H)
- Alarmanlage (H)

A2. Zugangskontrolle

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

- Benutzerkennung mit Passwort (H,S)
- Sichere Passworte (H,S)
- Firewall (H,S)
- Verschlüsselungsverfahren (S)
- Softwarebasierte Methoden zur Erhöhung der Anwendungssicherheit (S)
- Regelmäßige Unterweisung der Mitarbeitenden (S)

A3. Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems 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 (H,S)
- Benutzerkennung mit Passwort (H,S)
- Anwendung von Regeln und Verfahren zur Passwortsicherheit (S)
- Gesicherte Schnittstellen (H, S)
- Datenträgerverwaltung (H)
- Verschlüsselungsverfahren (H, S)

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 Verschlüsselungsverfahren):

- Sicherung bei der elektronischen Übertragung:
    - Verschlüsselung (H,S)
    - VPN (H, S)
    - Firewall (H,S)

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 (H,S)
- Benutzeridentifikation (H,S)

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 (H,S)
- Stichprobenprüfung (H,S)
- Kontrollrecht (H,S)
- Datenschutzvertrag nach Vorgaben §11 BDSG (H,S)

A7. Verfügbarkeitskontrolle

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

- Brandschutzmaßnahmen (H,S)
- Überspannungsschutz (H,S)
- Unterbrechungsfreie Stromversorgung (H,S)
- Klimaanlage (H)
- Festplattenspiegelung (H,S)
- Backupkonzept (H,S)
- Virenschutzkonzept (H,S)

A8. Zweckbindung

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

- Trennung von Produktiv- und Testsystemen (H,S)
- Getrennte Datenbanken (H,S)
- Mandantenspezifische Kennzeichnung der Datensätze (S)