

Inhaltsverzeichnis Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO der AFK-International GmbH

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)	2
als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)	2
Präambel	2
§ 1 Maßgebliche Begriffsbestimmungen	2
§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde	3
§ 3 Vertragsgegenstand	3
§ 4 Weisungsrecht	4
§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen	4
§ 6 Schutzmaßnahmen des Auftragnehmers	5
§ 7 Informationspflichten des Auftragnehmers	7
§ 8 Kontrollrechte des Auftraggebers	8
§ 9 Einsatz von Unterauftragsverarbeitern	9
§ 10 Unterstützung bei der Wahrung der Betroffenenrechte nach Art. 12 – 22 DS-GVO und der Einhaltung von Art. 32 – 36 DS-GVO	10
§ 11 Haftung	10
§ 12 Außerordentliches Kündigungsrecht	10
§ 13 Beendigung des Hauptvertrags	10
§ 14 Schlussbestimmungen	11
Anlagen	11
Anlage 1 – Beschreibung der Art der personenbezogenen Daten	12
Anlage 2 – Beschreibung der Kategorien betroffener Personen	12
Anlage 3 – Technische und organisatorische Maßnahmen des Auftraggebers	13
gemäß Art. 32 Abs. 1 DS-GVO und Art. 30 Abs. 2 Buchstabe d für Auftragsverarbeiter	13
Anlage 4 – Genehmigte Unterauftragsverarbeiter	19
Anlage 5 – Weisungsberechtigte Personen	20
Datum und Unterschriften	21

Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 EU-Datenschutz-Grundverordnung „DS-GVO“

zwischen

Firmierung, welche bei der Registrierung/im Administrationsportal angegeben wurde.

[Firmierung]

Anschrift, welche bei der Registrierung/im Administrationsportal angegeben wurde.

[Anschrift]

PLZ und Ort, welche bei der Registrierung/im Administrationsportal angegeben wurde.

[PLZ, Ort]

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und der

AFK-International GmbH

Colditzstraße 28

D – 12099 Berlin

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten (Folgend auch „Daten“ genannt). Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Maßgebliche Begriffsbestimmungen

- (1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- (2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- (3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen,

psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Die zuständige Aufsichtsbehörde für den Auftraggeber richtet sich nach seiner Hauptniederlassung.

(2) Die zuständige Aufsichtsbehörde für den Auftragnehmer ist:

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Bereitstellung einer Web Based Trainings-Plattform www.wbt-xray.de zur automatisierten Schulung von Teilnehmern in den Bereichen Luftsicherheit (Fracht- und Postkontrollen) u.ä. auf Grundlage des Dienstleistungs-, bzw. Kaufvertrages („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung) sowie den Nutzungsbedingungen und Allgemeinen Geschäftsbedingungen. Der Auftraggeber ist allein für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich.

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen und Weisungsempfänger ergeben sich aus **Anlage 5**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem jeweiligen Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten. Diese Daten umfassen die in **Anlage 1** aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten (nach Art. 9 DS-GVO).

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere die in **Anlage 3** aufgeführten Maßnahmen.

(3) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Beim Auftragnehmer ist als betrieblicher (externer) Datenschutzbeauftragter sowie als Ansprechpartner für den Datenschutz

Herr Patrick Bäcker
wavesun-technologies
Am Lerchenberg 15
63322 Rödermark
Tel.: 06074 / 370 9395

E-Mail: info@wavesun-technologies.de

benannt. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 und Art. 39 DS-GVO erfüllt werden. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(5) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO, schriftlich nach Art. 5 Abs. 1 DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(6) Verpflichtung zur Geheimhaltung nach § 203 StGB

Im Rahmen dieses Auftrages können auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 Strafgesetzbuch (StGB)) fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, dass ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Unterauftragnehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

Der Auftragnehmer ist berechtigt Unterauftragnehmer zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragnehmer zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist. Der Auftragnehmer wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. Der Auftragnehmer wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

Des Weiteren werden Unterauftragnehmer über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97 StPO informiert. Dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrecht von sogenannten mit-wirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

Der Auftraggeber weist den Auftragnehmer vor der Beauftragung auf die notwendige Verpflichtung nach § 203 und deren Umfang schriftlich hin. Wird nicht darauf hingewiesen, wird die Verpflichtung seitens des Auftragnehmers nicht vorgenommen.

(7) Verpflichtung zur Wahrung des Fernmeldegeheimnisses nach § 88 TKG

Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 88 Telekommunikationsgesetzes (TKG) zu verpflichten.

Der Auftraggeber weist den Auftragnehmer vor der Beauftragung auf die notwendige Verpflichtung nach § 88 TKG und deren Umfang schriftlich hin. Wird nicht darauf hingewiesen, wird die Verpflichtung seitens des Auftragnehmers nicht vorgenommen.

(8) Verpflichtung zur Wahrung von Geschäftsgeheimnissen und gesonderte Geheimhaltungsvereinbarungen

Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber mit vertraulichen Geschäftsgeheimnissen oder sonstigen geheimhaltungspflichtigen Informationen in Berührung kommt, verpflichtet er die hieran beteiligten Beschäftigten zur Wahrung von diesen Geschäftsgeheimnissen oder sonstigen geheimhaltungspflichtigen Informationen.

Der Auftraggeber weist den Auftragnehmer vor der Beauftragung auf die notwendige Verpflichtung zur Wahrung von Geschäftsgeheimnissen und deren Umfang schriftlich hin und übersendet ihm ggf. eine separate Geheimhaltungsvereinbarung. Wird nicht darauf hingewiesen, wird die Verpflichtung seitens des Auftragnehmers nicht vorgenommen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten (bei personenbezogenen Daten, welche den Auftraggeber betreffen) den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis von Verarbeitungstätigkeiten ist der zuständigen Aufsichtsbehörde auf Verlangen zur Verfügung zu stellen.

(8) An der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen der in dieser Vereinbarung vereinbarten technischen und organisatorischen Maßnahmen vor der Aufnahme der Datenverarbeitung und sodann regelmäßig (einmal jährlich) durchzuführen.

(2) Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen (bspw. durch den betrieblichen Datenschutzbeauftragten) vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten (vor Ort) selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang

durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(4) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(5) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(6) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 5, 6, 7 und 8 (sofern zutreffend) auf Verlangen nach.

§ 9 Einsatz von Unterauftragsverarbeitern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 4** genannten Unterauftragsverarbeiter durchgeführt, dem der Auftraggeber mit der Unterzeichnung dieses Vertrages zustimmt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverarbeitungsverhältnissen befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftraggeber kann innerhalb von 14 Tagen nach Kenntnisnahme des Einsatzes eines neuen Unterauftragsverarbeiters mit einer begründeten und verhältnismäßigen Stellungnahme widersprechen, bspw. wenn der Unterauftragsverarbeiter eine datenschutzrechtliche Nichtkonformität aufweist. Der Auftragnehmer ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Unterauftragsverarbeitern wahrnehmen kann. Sofern eine Einbeziehung von Unterauftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragsverarbeiter ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragsverarbeitern nachweisen. Der Auftragnehmer holt die Einwilligung des Auftraggebers nach § 3 Abs. 2 dieser Vereinbarung für eine Verlagerung in ein Drittland ein.

(2) Ein Unterauftragsverarbeitungsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen und

Bewachungsdienste ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverarbeitungsverhältnisse dar, soweit diese für IT-Systeme erbracht werden (und sofern dabei personenbezogene Daten erhoben, gespeichert und verarbeitet werden), die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Unterstützung bei der Wahrung der Betroffenenrechte nach Art. 12 – 22 DS-GVO und der Einhaltung von Art. 32 – 36 DS-GVO

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 – 22 (Unterstützung bei Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte) sowie zur Einhaltung nach den in Art. 32 – 36 DS-GVO genannten Pflichten. Darunter fällt insbesondere die angemessene (dem Auftrag unterliegende) Unterstützung bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO, den Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 und ggf. 34 DS-GVO, der ggf. erforderlichen Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und der Konsultation mit Aufsichtsbehörden nach Art. 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und teilt diesem auch das Betroffenenersuchen mit und wartet dessen Weisungen ab.

§ 11 Haftung

Es wird auf Art. 82 DS-GVO verwiesen.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann (gleiches gilt, bis auf Weisungen, auch andersrum). Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer, die nach dessen Löschkonzept regelmäßig vorgenommen werden. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen und Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1 – Beschreibung der Art der personenbezogenen Daten

Anlage 2 – Beschreibung der Kategorien betroffener Personen

Anlage 3 – Technische und organisatorische Maßnahmen „TOM´s“ des Auftragnehmers

Anlage 4 – Genehmigte Unterauftragsverarbeiter

Anlage 5 – Weisungsberechtigte und Weisungsempfänger

Datum und Unterschriften

Anlage 1 – Beschreibung der Art der personenbezogenen Daten

- Personenstamm-, Kommunikations- und Zahlungsdaten (Namen, Vornamen, Adressen, Telefonnummern, E-Mail-Adressen, Rechnungs-, Identifikations-, Legitimations- und Zuweisungsdaten sowie Freitext-Kommentare)
- Zertifikats- und Schulungsdaten von Teilnehmern
- Benutzernamen und Passwörter
- Schriftverkehr, welcher über die Web Based Trainings-Plattform läuft

Protokolldaten über die Nutzung der Web Based Trainings-Plattform, wie:

- Netzwerkverkehr (bspw. IP-Adressen) über die Nutzung und den Zugriff auf die Web Based Trainings-Plattform

Anlage 2 – Beschreibung der Kategorien betroffener Personen

- Administratoren
- Schulungsteilnehmer

Anlage 3 – Technische und organisatorische Maßnahmen des Auftraggebers

Beschreibung der technischen und organisatorische Maßnahmen (TOM's)

gemäß Art. 32 Abs. 1 DS-GVO und Art. 30 Abs. 2 Buchstabe d für Auftragsverarbeiter

Allgemeine Angaben			
Auftragsverarbeiter i.S.d. Art. 4 Abs. 8 DS-GVO	AFK-International GmbH		
Straße, Hausnummer	Colditzstraße 28		
Postleitzahl, Ort	12099, Berlin		
Datum	24.02.21		
zuletzt geprüft am:	17.03.2021		
Änderungshistorie			
Version	Stand	Bearbeiter	Änderung/Kommentar
01.00.00	24.02.2021	Patrick Bäcker (externer DSB)	Aufnahme der TOM's mit den Verantwortlichen der AFK-International GmbH
01.01.00	17.03.2021	Patrick Bäcker (externer DSB)	Finalisierung der TOM's mit den Verantwortlichen der AFK-International GmbH

HINWEIS: Die nachfolgenden technischen und organisatorischen Maßnahmen „TOM's“ finden Anwendung beim Zugriff/der Administration der AFK-International GmbH der Web Based Trainings-Plattform <https://www.wbt-xray.de>. Des Weiteren beschreiben diese TOM's den Schutz der personenbezogenen Daten innerhalb der AFK-International GmbH. Die für das Hosting, Programmier- und Datenbankarbeiten sowie die Pflege der Software und Systeme eingesetzten Dienstleister/Auftragsverarbeiter (siehe **Anlage 4**) der Web Based Trainings-Plattform erfüllen alle nach dem Stand der Technik vorgesehenen TOM's. Die TOM's der Dienstleister/Auftragsverarbeiter werden von der AFK-International GmbH regelmäßig überprüft und sichergestellt, dass diese ein gleichwertiges Schutzniveau zu den folgenden TOM's haben.

Gewährleistung der Vertraulichkeit der Systeme und Dienste

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Es soll der unautorisierte Zugang oder Zugriff auf personenbezogene Daten verhindert werden, beim Verantwortlichen selbst oder auf dem Transportweg zu Auftragsverarbeitern oder Dritten.

Dazu zählen u.a. Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle und Trennungskontrolle.

Zutrittskontrolle

Maßnahmen

- Manuelles Schließsystem
- Sicherheitsschlösser
- Dokumentierte Schlüsselausgabe
- Zutritt nur über besetzten Empfang möglich
- Besucher werden von Mitarbeitern begleitet
- Reinigungsdienst sorgfältig gewählt und zur Vertraulichkeit verpflichtet

Zugangs- und Zugriffskontrolle

Maßnahmen

- Login mit Benutzername + Passwort
- Vorgeschriebene Mindestlänge des Passworts ist 10 Zeichen
- Einhaltung der Passwortregeln wird technisch erzwungen
- Zwei-Faktor-Authentifizierung bei relevanten Systemen
- Verwenden von Passwortmanagern
- Server verfügen über Virenschutz
- Clients verfügen über Virenschutz
- Externe Datenzugriffe nur über Firewall
- Einsatz VPN bei Remote-Zugriffen
- Automatische Desktopsperrung erfolgt nach 10 Minuten
- Passwortvergabe über geregelten Prozess
- Passwortrichtlinie vorhanden
- Richtlinie zu Löschen und Vernichten
- Richtlinie zum Umgang mit Telefon, E-Mail und Internet
- Richtlinie zum Umgang mit mobilen Geräten
- Richtlinie zum Datenschutz in der Mobile- und Telearbeit
- Allgemeine Unternehmensrichtlinie zum Datenschutz

- Verbot der Nutzung privater Geräte
- Verschlüsselung von externen Datenträgern
- Verschlüsselung von Notebooks und Tablets
- Dokumentierte Berechtigungskonzepte
- Verwaltung der Benutzerrechte durch festgelegte Verantwortliche

Weitergabekontrolle

Maßnahmen

- Verschlüsselung von E-Mail-Anhängen mit vertraulichen personenbezogenen Daten
- Transportverschlüsselung von E-Mails (TLS)
- Externe Zugriffe über VPN
- Protokollierung der Zugriffe und Abrufe bei Datenübermittlungen
- Verwendung sicherer Transportbehälter (z.B. bei Transport von Backup-Platten)
- Datenübertragung über verschlüsselte Verbindungen wie sftp, https
- Dokumentation der Datenempfänger
- Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form, wo möglich
- Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen
- Nutzung von Signaturverfahren zur Authentifizierung bei Abruf/Übertragung

Trennungskontrolle

Maßnahmen

- Trennung von Produktiv- und Testsystemen
- Trennung von Entwicklungs- und Produktivnetzen
- Physikalische Trennung von relevanten Systemen (Datenbanken/Datenträger)
- Physikalische Trennung von relevanten Datenbanken
- Relevante Anwendungen sind mandantenfähig
- Steuerung von Mandantentrennung über Berechtigungskonzepte
- Steuerung von Mandantentrennung über Datenbankrechte

Gewährleistung der Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren. Kurz, personenbezogene Daten dürfen nicht (unbemerkt) geändert werden können.

Gewährleistung der Integrität

Maßnahmen

Protokollierung von Zugriffen auf Anwendungen in relevanten Systemen

Protokollierung von Eingabe, Änderung und Löschung von Daten in relevanten Systemen

Gewährleistung der Verfügbarkeit/Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit, Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von Daten, auch von im Auftrag verarbeiteten Daten, oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

Personenbezogene Daten sollen dauernd und uneingeschränkt verfügbar sein und insbesondere vorhanden sein, wenn sie gebraucht werden.

Verfügbarkeitskontrolle

Maßnahmen

Feuerlöscher im Serverraum

Temperaturüberwachung der Server

Keine wasserführenden Leitungen im Serverraum oder oberhalb des Serverraums

Wärmeabfuhr der Server gewährleistet

Einsatz von unterbrechungsfreier Stromversorgung für Server (USV)

RAID-System

Festplattenspiegelung

Regelmäßige ausgelagerte sichere offline Backups relevanter Daten und Systeme

Dokumentiertes Backup- und Recovery-Konzept

Kontrolle des Sicherungsvorgangs

Regelmäßige Tests zur Wiederherstellung von Daten und Systemen sowie Protokollierung der Ergebnisse

Auftragskontrolle

Maßnahmen

Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit

Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

Weisungen an den Auftragnehmer mindestens in Textform

Festlegung von weisungsberechtigten Personen

Festlegung der berechtigten weisungsempfangenden Personen

Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit und ggf. besondere Geheimhaltungspflichten

Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

Regelung zum Einsatz weiterer Unterauftragsverarbeiter

Sicherstellung der Vernichtung/Löschung von Daten nach Beendigung des Auftrags

Regelmäßige Überprüfung des Auftragnehmers und seiner Sicherheitsmaßnahmen

Kontrolle der Auftragsergebnisse durch den Auftraggeber

Gewährleistung der Belastbarkeit der Systeme

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder -abstürzen ist zu reduzieren.

Das bedeutet, Systeme und Dienste sind so auszulegen, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben.

Maßnahmen beziehen sich insbesondere auf Speicher-, Zugriffs- und Leitungskapazitäten.

Belastbarkeit der Systeme

Maßnahmen

Dokumentierter Prozess für Umgang mit Sicherheitsverletzungen

Monitoring der getroffenen Maßnahmen

Relevante Systeme sind skalierend

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Datenschutzmanagement

Maßnahmen

Datenschutzmanagementsystem (DSMS) besteht

Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz

Dokumentiertes Sicherheitskonzept

Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen

Dokumentierte Prozesse für Betroffenenanfragen (Auskunft, Löschung, Widerspruch, Änderung) sind vorhanden

Ein Datenschutzbeauftragter (DSB) ist benannt

Mitarbeiter sind zur Vertraulichkeit und auf besondere Geheimhaltungspflichten verpflichtet

Regelmäßige Datenschutz-Sensibilisierung der Mitarbeiter im jährlichen Turnus sowie zusätzlich bei speziellen Anlässen (Gesetzesänderungen etc.)

Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO wird bei Bedarf durchgeführt

Informationspflichten nach Art. 13 und 14 DS-GVO werden erfüllt

Dokumentierter Prozess zur Erkennung, Behandlung und Meldung von Datenschutzverletzungen

Dokumentation von Datenschutzverletzungen

Einbindung des Datenschutzbeauftragten bei Datenschutzverletzungen

Dokumentenname:

04.01.02 | AV-Vertrag AFK-International GmbH

Klassifizierung: 02 INTERN

Stand:

22.07.2021

Ver.: 01.01



Seite 17 von 21

© wavesun-technologies | Patrick Bäcker
Datenschutztechnische Betreuung
info@wavesun-technologies.de

Dokumentierter Prozess zur Nachbearbeitung von Datenschutzverletzungen

IT-Störungsmanagement

Maßnahmen

Dokumentierter Prozess zur Erkennung, Behandlung und Meldung von IT-Sicherheitsvorfällen

Dokumentation von Sicherheitsvorfällen

Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle

Dokumentierter Prozess zur Nachbearbeitung von Sicherheitsvorfällen

Anlage 4 – Genehmigte Unterauftragsverarbeiter

Die nachfolgenden Unternehmen sind genehmigte Unterauftragsverarbeiter im Sinne des § 9 dieses Vertrages:

Unterauftragsverarbeiter	Anschrift	Leistung
Scalingo SAS	15 avenue du Rhin 67100 Strasbourg, Frankreich	Hosting der Web Based Trainings-Plattform https://www.wbt-xray.de
Sascha Weidlich	Hans-Sachs-Straße 31a D – 65428 Rüsselsheim	Programmier- und Datenbankarbeiten sowie Pflege der Web Based Trainings-Plattform https://www.wbt-xray.de
Mailjet SAS	4, rue Jules Lefebvre 75009 Paris, Frankreich	Hosting und Versand von E-Mails, welche die Web Based Trainings-Plattform https://www.wbt-xray.de betreffen

Anlage 5 – Weisungsberechtigte Personen

(1) Weisungsberechtigte Personen des Auftraggebers sind:

Name:	Position:	E-Mail-Adresse:	Telefonnummer:
Name, welcher bei der Registrierung/im Administrationsportal	Position, welche bei der Registrierung/im	E-Mail-Adresse, welche bei der Registrierung/im Administrationsportal angegeben wurde.	Telefonnummer, welche bei der Registrierung/im Administrationsportal

(2) Weisungsempfänger beim Auftragnehmer sind

- Name:** Dennis Ellinghausen
Position: Geschäftsführer
E-Mail-Adresse: d.ellinghausen@afk-international.de
Telefonnummer: 030 / 76758090
- Name:** Nina Ellinghausen
Position: Geschäftsführerin
E-Mail-Adresse: n.ellinghausen@afk-international.de
Telefonnummer: 030 / 76758090
- Name:** Thomas Eslam
Position: Geschäftsführer
E-Mail-Adresse: t.eslam@afk-international.de
Telefonnummer: 030 / 76758090
- Name:** André Knoblauch
Position: Geschäftsführer
E-Mail-Adresse: a.knoblauch@afk-international.de
Telefonnummer: 030 / 76758090
- Name:** Marit Heinisch
Position: Sachbearbeiterin
E-Mail-Adresse: m.heinisch@afk-international.de
Telefonnummer: 030 / 76758090

Datum und Unterschriften

Elektronischer Abschluss nach Art. 28 Abs. 9 DS-GVO durch Anklicken der Checkbox. Dies wird systemseitig protokolliert.

.....
Ort, Datum

Der Vertrag tritt zum Zeitpunkt des Anklicken der Checkbox seitens des Auftraggebers in Kraft. Dies wird systemseitig protokolliert.

.....
Ort, Datum

Elektronischer Abschluss nach Art. 28 Abs. 9 DS-GVO durch Anklicken der Checkbox. Dies wird systemseitig protokolliert.

.....
Unterschrift (Auftraggeber)


gut beraten. gut geschult.
info@afk-international.de
Tel.: +49 (0) 30 / 7675809-0
.....
AFK International GmbH
Cordkatzstr. 28, 1007
12099 Berlin

Unterschrift (Auftragnehmer)