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

Vertrag zur Auftragsverarbeitung gemäß 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 Ziffer 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 Sicherungsmaßregeln 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. Gegenstand und Dauer sowie Art und Zweck der Verarbeitung

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Bereitstellung und des zugehörigen Supports einer Web-Plattform myqualityguard.de zum Management von Erinnerungen für ablaufende Dokumente bzw. Fristenverwaltung, der Ablage von zugehörigen Dokumenten, der Erstellung von Auditprotokollen sowie ergänzenden Leistungen und zukünftigen Plattformleistungen auf Grundlage der Allgemeinen Geschäftsbedingungen (myqualityguard.de/agb) sowie ggf. separaten Verträgen („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 sowie der Software- und Dienstleistungsbeschreibung auf myqualityguard.de. 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. Weisungen

(1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere auch 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 dokumentierter elektronischer Form 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 personenbezogenen 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 Schrift- oder 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 (Art. 28 Abs. 3 Satz 3 DS-GVO). 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 personenbezogenen Daten, Kategorien betroffener Personen

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

(2) Die Kategorien betroffener Personen sind 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 personenbezogenen Daten des Auftraggebers gemäß 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 13
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) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Personen vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. 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 zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 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.

(6) Verpflichtung zur Verschwiegenheit nach § 203 StGB

Sofern im Rahmen dieses Auftrages auch Daten verarbeitet werden, die unter ein Berufsgeheimnis (im Sinne von § 203 Strafgesetzbuch (StGB)) fallen, verpflichtet sich der Auftragnehmer, 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 mindestens in einem dokumentierten elektronischen Format 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 Unterauftragsnehmer 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 (Berufsgeheimnisträger) 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 in Schrift- oder Textform hin. Wird nicht darauf hingewiesen, wird die Verpflichtung seitens des Auftragnehmers nicht vorgenommen.

(7) Verpflichtung zur Wahrung des Fernmeldegeheimnisses nach § 3 TTDSG

Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich oder in einem dokumentierten elektronischen Format auf das Fernmeldegeheimnis i.S.d. § 3 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zu verpflichten.

Der Auftraggeber weist den Auftragnehmer vor der Beauftragung auf die notwendige Verpflichtung nach § 3 TTDSG und deren Umfang in Schrift- oder Textform 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 in Schrift- oder Texform 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, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten seitens des Auftragnehmers (bei personenbezogenen Daten, welche den Auftraggeber betreffen) sowie

Verletzung durch beim Auftragnehmer im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schrift- oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch eine 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 personenbezogenen 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 personenbezogenen 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 personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach Ziffer 6 Abs. 2, welche das zugesicherte Schutzniveau unterschreiten, 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, dass 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 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 (Terminvereinbarung – sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich scheint) zu den üblichen Geschäftszeiten (vor Ort) selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem unmittelbaren 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, schriftliche oder elektronisch dokumentierte 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.

9. Einsatz von Unterauftragsverarbeitern

(1) Die vertraglich vereinbarten Leistungen bzw. Teilleistungen werden unter Einschaltung der in **Anlage 4** genannten Unterauftragsverarbeiter durchgeführt, dem der Auftraggeber mit der Unterzeichnung / Bestätigung dieses Vertrages zustimmt.

(2) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverarbeitungsverhältnissen befugt (Art. 28 Abs. 2 Satz 1 DS-GVO - allgemeine Genehmigung). Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftraggeber kann innerhalb von 14 Tagen nach Kenntnisnahme des bevorstehenden Einsatzes eines neuen Unterauftragsverarbeiters mit einer begründeten und verhältnismäßigen Stellungnahme Einspruch erheben (Art. 28 Abs. 2 Satz 2 DS-GVO), bspw. wenn der Unterauftragsverarbeiter eine datenschutzrechtliche Nichtkonformität aufweist.

(3) Der Auftragnehmer ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DS-GVO festgelegten Pflichten auferlegt sind. 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 holt die Einwilligung des Auftraggebers nach Ziffer 3 Abs. 2 dieser Vereinbarung für eine Verlagerung in ein Drittland ein.

(4) 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 den technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO, der Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 und 34 DS-GVO, der ggf. erforderlichen Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und der ggf. erforderlichen Konsultation mit Aufsichtsbehörden nach Art. 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner personenbezogenen 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 personenbezogener 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 personenbezogenen 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 personenbezogenen 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 personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schrift- oder Textform. 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- und Kommunikationsdaten (Namen, Vornamen, Geburtsdatum, Adressen, Telefonnummern, E-Mail-Adressen, Positionen/Funktionen, Standort/Niederlassung, Abteilung, Freitext-Kommentare, Dateien jeglicher Art wie Zertfikate, Nachweise u.ä., **bei denen auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DS-GVO enthalten sein können**)
- Benutzernamen und Passwörter (für den Login)
- Schriftverkehr, welcher über die Web-Plattform läuft (bspw. E-Mail-Versand)

Protokolldaten über die Nutzung der Web-Plattform, wie:

- Netzwerkverkehr (bspw. IP-Adressen, Zeitpunkt des Zugriffs, verwendeter Browser und Version) über die Nutzung und den Zugriff auf die Web-Plattform, welcher für die Herstellung einer Verbindung und der Darstellung von Inhalten sowie zur Gewährleistung der Systemsicherheit und weiteren administrativen Zwecken notwendig ist.

Anlage 2 – Beschreibung der Kategorien betroffener Personen

- Kunden
- Beschäftigte
- Dienstleister
- Lieferanten
- Geschäftspartner
- Benutzer

Beschreibung der technischen und organisatorische Maßnahmen (TOM´s)

gemäß Art. 30 Abs. 2 lit. d und Art. 32 Abs. 1 DS-GVO 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	**15.11.2023**
zuletzt geprüft am:	**15.11.2023**

Änderungshistorie			
Version	**Stand**	**Bearbeiter**	**Änderung/Kommentar**
01.00.00	**15.11.2023**	**Patrick Bäcker (externer DSB)**	**Aufnahme der TOM´s mit den Verantwortlichen der AFK-International GmbH**
01.01.00	**15.11.2023**	**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-Plattform https://www.myqualityguard.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-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 vergleichbar angemessenes Schutzniveau zu den folgenden TOM´s haben.

A. Gewährleistung der Vertraulichkeit

(gemäß Art. 32 Abs. 1 lit. b DS-GVO)

Erläuterung: *Unbefugten wird der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen von AFK, mit denen personenbezogene Daten verarbeitet werden mit den folgenden Maßnahmen verwehrt. Auch physische Unterlagen/Dokumente mit personenbezogenen Daten werden mit den folgenden Maßnahmen geschützt. Es soll damit der unautorisierte Zugang und Zugriff auf personenbezogene Daten verhindert werden.*

A.1.1 Zutrittskontrolle

Erläuterung: *Unter diesem Punkt wird aufgelistet, wie seitens AFK Unbefugten der Zutritt zu Datenverarbeitungsanlagen und physikalischen Unterlagen/Datenträgern verwehrt wird.*

Maßnahmen
☒ Elektronisches Schließsystem für alle Büroräume
☒ Manuelles Schließsystem mit mindestens Profilzylinderschlössern für alle weiteren Räume
☒ Dokumentierte Schlüsselausgabe
☒ Zutritt nur über besetzten Empfang möglich
☒ Besucher werden von Mitarbeitern begleitet
☒ Reinigungsdienst sorgfältig gewählt und zur Vertraulichkeit verpflichtet

A.1.2 Zugangskontrolle

Erläuterung: *Hierunter werden die Schutzmaßnahmen von AFK aufgelistet, welche verhindern, dass Datenverarbeitungssysteme und physikalische Unterlagen/Datenträger von Unbefugten genutzt werden können.*

Maßnahmen
☒ Login mit Benutzername + Passwort
☒ Vorgeschriebene Mindestlänge des Passworts ist 10 Zeichen
☒ Einhaltung der Passwortregeln wird technisch erzwungen
☒ Zwei-Faktor-Authentifizierung bei relevanten Systemen/Anwendungen/Diensten
☒ Verwenden von Passwortmanagern
☒ Server verfügen über Virenschutz
☒ Clients verfügen über Virenschutz
☒ Externe Datenzugriffe nur über Firewall
☒ Einsatz von VPN oder Tools mit Ende-zu-Ende-Verschlüsselung bei Remote-Zugriffen
☒ Automatische Bildschirmsperre erfolgt nach 10 Minuten
☒ Benutzer- und Passwortvergabe (Zuweisung, Änderung und Entzug) über geregelten Prozess
☒ Passwortrichtlinie vorhanden
☒ Richtlinie zu Löschen und Vernichten
☒ Richtlinie zum Umgang mit E-Mail, Internet und Telefon sowie der Regelung von privater und geschäftlicher Nutzung

☒ Richtlinie zum Umgang mit mobilen Geräten und personenbezogenen Daten/Unterlagen in der Mobile- und/oder Telearbeit
☒ Allgemeine Unternehmensrichtlinie zum Datenschutz
☒ Verbot der Nutzung privater Geräte

A.1.3 Zugriffskontrolle

Erläuterung: *Unter diesem Punkt wird aufgelistet, wie AFK gewährleistet, dass nur autorisierte Personen Zugriff auf die Ressourcen erhalten bzw. wie das unbefugte Lesen, Kopieren, Verändern oder Entfernen innerhalb von Systemen/Anwendungen/Diensten verhindert wird.*

Maßnahmen
☒ Technisch umgesetzte Berechtigungskonzepte für relevante Systeme/Anwendungen/Dienste
☒ Verwaltung der Benutzerrechte durch festgelegte Verantwortliche
☒ Minimale Anzahl an Administratoren
☒ Keine administrativen Kennungen für Nutzer, die keine administrativen Tätigkeiten ausführen
☒ Regelmäßige Überprüfung der Zugangs- und Zugriffsberechtigungen nach betrieblicher Notwendigkeit
☒ Aktenvernichter (mit mind. Sicherheitsstufe P-3 nach DIN 66399)

A.1.4 Trennungskontrolle

Erläuterung: *Die Trennungskontrolle bedeutet, dass seitens AFK erhobene Daten für verschiedene Zwecke getrennt verarbeitet werden. Auf diese Weise soll u.a. das Entstehen neuer Verarbeitungszwecke verhindert werden, die den betroffenen Personen unbekannt ist. Folgend werden die getroffenen Maßnahmen zur Trennungskontrolle aufgelistet.*

Maßnahmen
☒ Trennung von Produktiv- und Testsystemen
☒ Trennung von Entwicklungs- und Produktivnetzen
☒ Physikalische/virtuelle Trennung von relevanten Systemen/Datenbanken/Datenträgern
☒ Relevante Anwendungen sind mandantenfähig
☒ Steuerung von Mandantentrennung über Berechtigungskonzepte oder über Datenbankrechte

A.2.1 Verschlüsselung

(gemäß Art. 32 Abs. 1 lit. a DS-GVO)

Erläuterung: *Hierunter werden die Schutzmaßnahmen von AFK, welche die Verschlüsselung von Daten und (auf) Datenträgern gewährleisten aufgelistet.*

Maßnahmen
☒ Verschlüsselung von externen Datenträgern
☒ Verschlüsselung von Notebooks und Tablets

A.2.2 Pseudonymisierung

(gemäß Art. 32 Abs. 1 lit. a DS-GVO)

Erläuterung: *Die Anonymisierung wird bspw. für Daten(-sätze) verwendet, welche nach dem Ablauf der Zweckbindung in Ihrem Wert, jedoch nicht mehr personenbezogenen beibehalten werden sollen. Die Pseudonymisierung i.S.d. Art. 4 Abs. 5 DS-GVO*

bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, dass diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr spezifischen Personen zugeordnet werden können

Maßnahmen

☒ Derzeit keine Anonymisierung oder Pseudonymisierung eingesetzt, aufgrund von Nichtnotwendigkeit für weiterverarbeitende Zwecke

☒ Sollte zukünftig eine Anonymisierung oder Pseudonymisierung geplant sein, erfolgt bspw. die Trennung der Zuordnungsdaten und deren Aufbewahrung in getrennten, abgesicherten und verschlüsselten Systemen

B. Gewährleistung der Integrität

(gemäß Art. 32 Abs. 1 lit. b DS-GVO)

Erläuterung: *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 zu verarbeitenden personenbezogenen Daten ist zu reduzieren. Kurz, personenbezogene Daten dürfen bei AFK nicht (unbemerkt) geändert werden können.*

B.1 Weitergabekontrolle

Erläuterung: *Die Weitergabekontrolle bezieht sich auf den Verkehr von Daten und zeigt die Schutzmaßnahmen von AFK hierfür auf bzw. wie das unbefugte Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindert wird.*

Maßnahmen

☒ Verschlüsselung von E-Mail-Anhängen mit vertraulichen personenbezogenen Daten

☒ Transportverschlüsselung von E-Mails (TLS)

☒ Einsatz von VPN oder Tools mit Ende-zu-Ende-Verschlüsselung bei Remote-Zugriffen

☒ 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

☒ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen

☒ Nutzung von Signaturverfahren zur Authentifizierung bei Abruf/Übertragung

B.2 Eingabekontrolle

Erläuterung: *Hierunter wird aufgelistet, wie seitens AFK nachträglich festzustellen ist, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.*

Maßnahmen

☒ Protokollierung von Zugriffen auf relevante Systeme/Anwendungen/Dienste

☒ Protokollierung von Eingabe, Änderung und Löschung von Daten in relevanten Systemen/Anwendungen/Diensten

☒ Manuelle oder automatisierte Kontrolle der Protokolle

☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

☒ Klare Zuständigkeiten für Löschungen

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

(gemäß Art. 32 Abs. 1 lit. b und c DS-GVO)

Erläuterung: *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 bei AFK dauernd und uneingeschränkt verfügbar sein und insbesondere vorhanden sein, wenn sie gebraucht werden.

C.1 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
☒ Wirksamer, intern allen Beschäftigten bekannter Notfallplan bei IT-Vorfällen
C.2 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

D. Gewährleistung der Belastbarkeit der Systeme

(gemäß Art. 32 Abs. 1 lit. b DS-GVO)

Erläuterung: *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 verarbeiteten Daten oder des unbefugten Zugangs zu verarbeiteten Daten aufgrund von Systemüberlastungen oder -abstürzen ist zu reduzieren.*
Das bedeutet, AFK legt Systeme und Dienste wie folgend aufgelistet so aus, dass auch punktuell hohe Belastungen oder hohe

Dauerbelastungen von Verarbeitungen leistbar bleiben.

Maßnahmen

- ☒ Dokumentierter Prozess für den Umgang mit IT-Sicherheitsverletzungen
- ☒ Monitoring der getroffenen Maßnahmen
- ☒ Relevante Systeme sind skalierend

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

(gemäß Art. 32 Abs. 1 lit. d DS-GVO)

Erläuterung: *AFK betreibt die folgend aufgelisteten Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Datenschutzmanagement

Maßnahmen

- ☒ Regelmäßige Überprüfung der Aktualität und Wirksamkeit der technischen und organisatorischen Maßnahmen
- ☒ Ein Datenschutzmanagementsystem (DSMS) besteht
- ☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- ☒ Datenschutzrechtliche und datenschutztechnische Vorabkontrollen neuer Verarbeitungstätigkeiten
- ☒ Dokumentierte technischen und organisatorischen Maßnahmen
- ☒ Dokumentierte Prozesse für Betroffenenersuchen sind vorhanden
- ☒ Ein Datenschutzbeauftragter (DSB) ist benannt
- ☒ Mitarbeiter sind zur Vertraulichkeit und auf besondere Geheimhaltungspflichten verpflichtet
- ☒ Regelmäßige Datenschutz-Unterweisung der Mitarbeiter im jährlichen Turnus sowie zusätzlich bei speziellen Anlässen (Gesetzesänderungen etc.)
- ☒ Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO wird bei Bedarf durchgeführt
- ☒ Informationspflichten gemäß 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
- ☒ Dokumentierter Prozess zur Nachbearbeitung von Datenschutzverletzungen

F. Auftragskontrolle

Erläuterung: Verfahren und Maßnahmen, welche AFK einsetzt, um insb. Dienstleister und Lieferanten (Auftragsverarbeiter), welche Daten im Auftrag nach Weisung verarbeiten zu kontrollieren, um den Schutz personenbezogener Daten sicherzustellen.

Maßnahmen

- ☒ Auswahl der Auftragnehmer unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit

☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO
☒ Sofern zutreffend - Sicherstellung nach Art. 44 ff. DS-GVO von technisch und vertraglich abgesicherten Übermittlungen personenbezogener Daten in Drittländer
☒ Weisungen an den Auftragnehmer mindestens in Textform
☒ Festlegung von weisungsberechtigten Personen
☒ Festlegung der berechtigten weisungsempfangenden Personen
☒ Sicherstellung der Verpflichtung der Beschäftigten der Auftragsverarbeiter zur Vertraulichkeit und auf besondere Geheimhaltungspflichten
☒ Vereinbarung wirksamer Kontrollrechte gegenüber Auftragsverarbeitern
☒ 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
☒ Bei Fernwartungen durch externe Dienstleister werden diese systemseitig und/oder durch den Dienstleister protokolliert; Zugriffe werden nur bei Notwendigkeit freigegen und nach Möglichkeit von einem Beschäftigten am Bildschirm verfolgt – Dauerzugriffe nur bei Notwendigkeit und Festlegung schriftlicher Sicherheitsregelungen
G. Datenschutzfreundliche Voreinstellungen ***(gemäß Art. 25 DS-GVO)*** ***Erläuterung:*** *Verfahren und Maßnahmen, welche AFK einsetzt, um bereits bei der Erhebung von personenbezogenen Daten die Grundsätze der DS-GVO (insb. der Datensparsamkeit) einzuhalten.*
Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich
☒ Die Einstellungen in Datenverarbeitungssysteme, Anwendungen und Diensten sind datensparsam vorgenommen; neue Verarbeitungstätigkeiten werden im Rahmen von datenschutzrechtlichen und datenschutztechnischen Vorabkontrollen überprüft

Anlage 4 – Genehmigte Unterauftragsverarbeiter

Die nachfolgenden Unternehmen sind genehmigte Unterauftragsverarbeiter nach Ziffer 9 Abs. 1 dieser Vereinbarung:

Unterauftragsverarbeiter	**Anschrift**	**Leistung und Datenverarbeitungsort**
Webentwicklung Düngel - Inh. Christoph Düngel	Eschenweg 1B, 14547 Beelitz, Deutschland	Last-Level-Support der Web-Plattform https://www.myqualityguard.de, inklusive Fernwartung Die Datenverarbeitung findet innerhalb des EWR / der EU statt.
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Deutschland	Hosting der Web-Plattform https://www.myqualityguard.de Die Datenverarbeitung findet innerhalb des EWR / der EU statt.
STRATO AG	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Hosting des Mailing-Servers für Ausgangsmails und der Domain von https://www.myqualityguard.de Die Datenverarbeitung findet innerhalb des EWR / der EU statt.

Anlage 5 – Weisungsberechtigte und Weisungsempfänger

(1) Weisungsberechtigte Personen des Auftraggebers sind:

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

(2) Weisungsempfänger beim Auftragnehmer sind

1. **Name:** Dennis Ellinghausen

   Position: Geschäftsführer

   E-Mail-Adresse: datenschutz@afk-international.de

   Telefonnummer: 030 / 76758090

2. **Name:** Nina Ellinghausen

   Position: Geschäftsführerin

   E-Mail-Adresse: datenschutz@afk-international.de

   Telefonnummer: 030 / 76758090

3. **Name:** Thomas Eslam

   Position: Geschäftsführer

   E-Mail-Adresse: datenschutz@afk-international.de

   Telefonnummer: 030 / 76758090

4. **Name:** André Knoblauch

   Position: Geschäftsführer

   E-Mail-Adresse: datenschutz@afk-international.de

   Telefonnummer: 030 / 76758090

Datum und Unterschriften

Elektronischer Abschluss nach Art. 28 Abs. 9 DS-GVO durch Anklicken bzw. Aktivierung der Checkbox im Registrierungsformular. **Dies wird systemseitig protokolliert.** **_____** **Ort, Datum**	**Der hiesige AV-Vertrag tritt zum Zeitpunkt des Anklickens bzw. Aktivierung der Checkbox und Absendung des Registrierungsformulars seitens des Auftraggebers in Kraft.** **Dies wird systemseitig protokolliert.** **_____** **Ort, Datum**
Elektronischer Abschluss nach Art. 28 Abs. 9 DS-GVO durch Anklicken bzw. Aktivierung der Checkbox im Registrierungsformular. **Dies wird systemseitig protokolliert.** **_____** **Name + Unterschrift (Auftraggeber)**	Dennis Ellinghausen afk gut beraten - gut geschult info@afk-international.de AFK-International GmbH Colditzstr. 28, Bau 7 12099 Berlin **_____** **Name + Unterschrift (Auftragnehmer)**