1. Geltung und Anwendungsbereich

Falls bei der Inanspruchnahme der vertragsgegenständlichen Leistungen von der **CERTNET GmbH, Forstfeldstr. 2, 34123 Kassel**, nachfolgend CERTNET genannt, eine Verarbeitung von personenbezogenen Daten im Auftrag des Kunden als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO erfolgt, vereinbaren die Parteien nach Maßgabe der Allgemeinen Geschäftsbedingungen nachfolgende Vereinbarung über die Verarbeitung personenbezogener Daten (AVV) im Sinne des Art. 28 Abs. 3 DSGVO. Diese unterliegt den nachstehenden Bestimmungen, welche den Allgemeinen Geschäftsbedingungen, die im Übrigen gelten, vorrangig sind.

2. Begriffsbestimmungen

2.1 ***Verantwortlicher*** ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

2.2 ***Auftragsverarbeiter*** ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

2.3 ***Personenbezogene Daten*** sind gem. Art. 4 Abs. 1 DSGVO 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.

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

2.5 ***Verarbeitung*** ist gem. Art. 4 Abs. 2 DSGVO 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.

2.6 ***Aufsichtsbehörde*** ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

3. Angabe der zuständigen Datenschutz-Aufsichtsbehörde; Datenschutzbeauftragter

3.1 Zuständige Aufsichtsbehörde für CERTNET (nachfolgend auch „Auftragsverarbeiter“) ist der Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (https://datenschutz.hessen.de).

3.2 Der Kunde (nachfolgend auch „Verantwortlicher“) und CERTNET sowie gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

3.3 Datenschutzbeauftragter von CERTNET ist Jonas Stellmacher, zu kontaktieren über info@certnet.de.

4. Vertragsgegenstand

4.1 CERTNET unterstützt den Verantwortlichen durch Technischen Support und Beratungsleistungen, dabei teilweise durch den Einsatz von AnyDesk Fernwartungssoftware nach Maßgabe der Allgemeinen Geschäftsbedingungen. Dabei erhält CERTNET Zugriff auf personenbezogene Daten (nachfolgend auch nur „Daten“) und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Umfang und Zweck der Datenverarbeitung durch CERTNET als Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dem Verantwortlichen obliegt indes die Beurteilung der Zulässigkeit der Datenverarbeitung.

4.2 CERTNET bleibt es vorbehalten, die Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zu Zwecken der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung der nach Maßgabe des Hauptvertrages vereinbarten Leistungen zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Daten nicht mehr als Daten im Sinne dieses Vertrages gelten.

4.3 CERTNET darf die Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen dies gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

4.4 Die Bestimmungen dieser Bedingungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei welchen CERTNET und seine Beschäftigten oder durch CERTNET Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für diesen erhoben wurden.

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

4.6 Die Verarbeitung der Daten durch CERTNET außerhalb des Gebiets der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens erfolgt nur unter den Voraussetzungen von Kapitel 5 Art. 44 ff. DSGVO ().

5. Verantwortlichkeit und Weisungsrecht

5.1 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis zueinander allein verantwortlich.

5.2 CERTNET darf Daten, auch für den Fall einer Verwendung anonymisierter Daten, nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird CERTNET durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

5.3 Die Weisungen des Verantwortlichen werden anfänglich durch diese Ergänzenden Bedingungen festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst insbesondere Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten, sofern keine berechtigten vertraglichen Interessen oder gesetzliche Bestimmungen dem entgegenstehen.

5.4 Die weisungsberechtigte Person des Kunden als Verantwortlichen ergeben sich aus dessen Angaben im Rahmen von Registrierungs- oder Supportprozessen bzw. den aktuellen Angaben des Kunden**.** Bei einem Wechsel oder einer längerfristigen

Verhinderung der benannten Personen ist CERTNET unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

5.5 Alle erteilten Weisungen sind sowohl von CERTNET als auch vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

5.6 Ist CERTNET der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat CERTNET den Verantwortlichen unverzüglich darauf hinzuweisen. CERTNET ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. CERTNET darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

5.7 CERTNET erwirbt an den Daten keine Rechte und ist für die Dauer des Hauptvertrages auf Verlangen des Verantwortlichen jederzeit auf erstes Anfordern zur Herausgabe ggf. gespeicherter Daten in einer für den Verantwortlichen lesbaren und weiterverarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf die Daten und die dazugehörigen Datenträger sind ausgeschlossen.

6. Art der verarbeiteten Daten, Kreis der Betroffenen

6.1 Im Rahmen der Durchführung des Hauptvertrags erhält CERTNET, soweit erforderlich, Zugriff auf folgende u. a. personenbezogene Daten, die verarbeitet werden:

(i) Bestandsdaten (Namen, Adressen, Geschlecht, Firma, Standort),
(ii) Zahlungsdaten (Bankverbindungen, Rechnungen, Zahlungshistorie),
(iii) Kontaktdaten (E-Mail, Telefonnummern),
(iv) Vertrags- und Kundenkontodaten (Vertragsgegenstand, Lizenzart, Laufzeit, Kundenkategorie, Kunden-ID, Lizenzschlüssel, Login-Daten),
(v) Der Verwendung der AnyDesk Fernwartungssoftware, die von CERTNET für Support- und Betreuungszwecke eingesetzt wird, unterliegt der AVV von AnyDesk und ist unter https://anydesk.com/de/agb abrufbar.

6.2 Folgende Kategorien von Personen sind von der Verarbeitung betroffen: (i) Kunden, Geschäftspartner, Interessenten, Benutzer der zu betreuenden Software.

7. Schutzmaßnahmen des Auftragsverarbeiters

7.1 CERTNET ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen 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.

7.2 CERTNET wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. CERTNET trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten gem. Art. 32 DSGVO unter Berücksichtigung der gesetzlichen Vorgaben nach Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO, d. h. mindestens die in Anlage 1 aufgeführten Maßnahmen, welche zu dokumentieren sind und Folgendes einschließen:

(i) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
(ii) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt CERTNET vorbehalten, wobei sichergestellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

7.3 Den bei der Datenverarbeitung durch CERTNET beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. CERTNET 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 DSGVO) 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 CERTNET bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

8. Informations- und Mitwirkungspflichten von CERTNET

8.1 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen von CERTNET, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch CERTNET, bei CERTNET im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird CERTNET den Verantwortlichen unverzüglich in Schriftform oder Textform informieren.
Dasselbe gilt für Prüfungen von CERTNET durch die Datenschutz Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

(i) 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;

(ii) eine Beschreibung der von CERTNET ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

CERTNET trifft darüber hinaus im Falle unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

8.2 CERTNET ist verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit die Daten von einer Verletzung nach Absatz 1 betroffen sind.

8.3 Sollten die Daten bei CERTNET durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat CERTNET den Verantwortlichen unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. CERTNET wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Verantwortlichen liegen.

8.4 Über wesentliche Änderung der Sicherheitsmaßnahmen nach Ziffer 7.1 hat CERTNET den Verantwortlichen unverzüglich zu unterrichten.

8.5 Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

8.6 CERTNET führt ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, welches alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Verantwortlichen auf Anforderung zur Verfügung zu stellen.

8.7 An der Erstellung des Verfahrensverzeichnisses durch den Verantwortlichen hat CERTNET im angemessenen Umfang mitzuwirken. Er hat dem Verantwortlichen die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

9. Kontrollrechte des Verantwortlichen

9.1 Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von CERTNET. Hierfür kann er z. B. Auskünfte von CERTNET einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen gemäß Art. 42 DSGVO oder internen Prüfungen vorlegen lassen, oder die technischen und organisatorischen Maßnahmen von CERTNET nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu CERTNET steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe von CERTNET dabei nicht unverhältnismäßig stören.

9.2 CERTNET verpflichtet sich, dem Verantwortlichen 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 erforderlich sind.

9.3 Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es CERTNET mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche feststellt, hat er CERTNET unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche CERTNET die notwendigen Verfahrensänderungen unverzüglich mit.

9.4 CERTNET stellt dem Verantwortlichen auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

9.5 CERTNET weist dem Verantwortlichen die Verpflichtung der Mitarbeiter nach Ziffer 7.3 auf Verlangen nach.

9.6 Im Falle der Verarbeitung von Daten im Unterauftrag (d.h. der Kunde ist bereits Auftragsverarbeiter eines Dritten; CERTNET als Subunternehmer) verpflichtet sich der Verantwortliche, die vorstehend beschriebenen Kontrollrechte auch dem Dritten direkt einzuräumen.

10. Einsatz von Subunternehmern

10.1 Die vertraglich vereinbarten Leistungen des Hauptvertrages werden bedarfsweise unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt.

10.2 CERTNET ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmer-verhältnis“) befugt. CERTNET setzt den Verantwortlichen hierüber vorab in Textform in Kenntnis, womit der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen im Einzelfall Einspruch zu erheben. Ein Einspruch darf vom Verantwortlichen nur aus wichtigem, CERTNET nachzuweisenden Grund erhoben werden. Soweit der Verantwortliche nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung in Textform Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Verantwortliche Einspruch, ist CERTNET berechtigt, den Hauptvertrag sowie diese ergänzenden Bedingungen unbenommen der Kündigungsregelung der Allgemeinen Geschäftsbedingungen mit einer Frist von zwei Wochen zum Monatsende außerordentlich zu kündigen. In diesem Fall wird dem Kunden eine auf die Vertragslaufzeit bezogene Vergütung *pro rata temporis* erstattet; weitergehende Ansprüche des Kunden bestehen insoweit nicht.

10.3 CERTNET ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen, und hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Verantwortliche seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Der Vertrag mit dem Subunternehmer muss

schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

10.4 Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat CERTNET sicherzustellen, dass die gesetzlichen Voraussetzungen hierfür gemäß Art. 44 ff. DSGVO vorliegen. Soweit im Hinblick auf ein Drittland kein Beschluss nach Art. 45 Abs. 3 DSGVO vorliegt, erfolgt eine Datenverarbeitung durch den Subunternehmen nur, sofern durch geeignete Garantien ein angemessenes Datenschutzniveau gewährleistet ist. Ein angemessener Schutz der übermittelten Daten wird durch den Abschluss der (von der Europäischen Kommission vorgegebenen) Standardvertragsklauseln sowie entsprechenden organisatorischen und technischen Maßnahmen sichergestellt. Die Einhaltung der Standardvertragsklauseln sowie der organisatorischen und technischen Maßnahmen wird regelmäßig überprüft. CERTNET wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

10.5 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn CERTNET Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die CERTNET für den Verantwortlichen erbringt, und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmer-verhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

11. Anfragen und Rechte Betroffener

11.1 CERTNET unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 DSGVO sowie Art. 32 und 36 DSGVO.

11.2 Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber CERTNET geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

12. Haftung

12.1 Der Verantwortliche und CERTNET haften gegenüber Betroffenen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

12.2 Im Innenverhältnis der Parteien gelten, soweit nicht ausdrücklich anderweitig vereinbart, die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen CERTNET geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Verantwortlichen gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Verantwortliche CERTNET von diesen Ansprüchen auf erstes Anfordern frei.

12.3 Der Verantwortliche verpflichtet sich überdies, CERTNET auch von allen etwaigen Geldbußen, die gegen CERTNET verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Verantwortliche Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

13. Außerordentliches Kündigungsrecht

13.1 Beide Parteien können den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der die jeweils andere Partei ihre Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder CERTNET eine Weisung des Verantwortlichen nicht ausführen kann oder will.

13.2 Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt die eine Partei der jeweils anderen eine angemessene Frist, innerhalb welcher diese den Verstoß abstellen kann.

14. Datenlöschung

14.1 CERTNET wird die Daten nach Beendigung des Hauptvertrages löschen, sofern für CERTNET nicht gesetzlich eine Verpflichtung zur weiteren Speicherung der Daten besteht.

14.2 Dokumentationen, die zum Nachweis der auftrags- und ordnungsgemäßen Verbreitung der Daten dienen, dürfen durch CERTNET auch nach dem Ende des Hauptvertrags zu Beweiszwecken aufbewahrt werden.

15. Vergütung

Die Vergütung für die Verarbeitung der personenbezogenen Daten im Rahmen dieser Vereinbarung ist, soweit nicht ausdrücklich anderweitig vereinbart, in der Vergütung für die im Rahmen des Hauptvertrages erbrachten Leistungen enthalten.

16. Schlussbestimmungen

16.1 Sollten sich die im vorliegenden Vertragswerk referenzierten Verweise auf gesetzliche Bestimmungen während der Laufzeit des Vertrages ändern, gelten diese verweise auch für die jeweiligen Nachfolgebestimmungen.

16.2 CERTNET ist berechtigt, diese Vereinbarung zu ändern. CERTNET wird den Verantwortlichen über die geplante Änderung mindestens 30 Tage vor deren Wirksamwerden informieren. Die Änderung wird Vertragsbestandteil, sofern der Verantwortliche nicht innerhalb von 30 Tagen nach Erhalt der Änderungsmitteilung widerspricht. Widerspricht der Verantwortliche der Änderung, besteht diese Vereinbarung zu den bestehenden Bedingungen fort. Als Änderung im vorgenannten Sinne gilt nicht die Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern.

16.3 Sollten dagegen 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.

16.4 Diese Vereinbarung unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland.

16.5 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist der Geschäftssitz von CERTNET in Kassel, sofern der Verantwortliche Kaufmann oder juristische Person des öffentlichen Rechts ist oder keinen allgemeinen Gerichtsstand im Gebiet der Bundesrepublik Deutschland hat. CERTNET ist berechtigt, auch an jedem anderen gesetzlich vorgesehenen Gerichtsstand zu klagen.

17. Anlagen

Anlage 1: Technische und organisatorische Maßnahmen
Anlage 2: Genehmigte Subunternehmer

Anlage 1
Technische und organisatorische Maßnahmen

Maßnahmenforderung	gesetzliche Anforderung	Umsetzung in der Praxis
Zutrittskontrolle	Unbefugten den Zutritt zu DV-Anlagen verwehren	Das Betriebsgebäude ist außerhalb der Geschäftszeiten stets verschlossen. Zu den Büroräumen besteht ein Zugang, der eingesehen werden kann. Dritte haben zu den Räumlichkeiten keinen Zutritt. Besucher werden von Mitarbeiter*innen in Empfang genommen und ihre Anmeldung wird kontrolliert. Über ein Schließsystem wird durch verschiedene Berechtigungsstufen gewährleistet, dass Mitarbeiter neben den allgemeinen Bereichen nur Räume betreten können, für diese sie speziell berechtigt wurden.
Zugangskontrolle	Nutzung von DV-Anlagen durch Unbefugte verhindern	Alle Rechner der Mitarbeiter*innen verfügen über einen Virenschutz. Um Zugang zu Datenverarbeitungssystemen zu bekommen, müssen sich Mitarbeiter*innen mindestens mit Benutzererkennung und Passwort identifizieren. Die Bildschirme werden automatisch nach der Inaktivität gesperrt. Jeder Mitarbeiter hat ein eigenes Benutzerkonto mit individuellen Zugriffrechten. Die Anzahl der Login-Versuche werden protokolliert und nach Überschreitung der maximalen Anzahl fehlerhafter Login-Versuche, wird das Benutzerkonto gesperrt. Eine Entsperrung ist nur durch eine Administration nach Authentifikation des Mitarbeiters/in, möglich. Nach der Entsperrung wird der Anwender aufgefordert ein persönliches Passwort zu vergeben. Mobiles Arbeiten für Mitarbeiter*innn ist durch VPN (bzw. gesicherten Cloud-Zugriff) gesichert. Alle Endgeräte und Datenträger sind, wenn möglich, verschlüsselt. Die Firmennetzwerke sind durch Firewalls abgesichert. Die Netzwerksegmente sind durch eine Firewall getrennt. Die Firewall-

Maßnahmenforderung	gesetzliche Anforderung	Umsetzung in der Praxis
		Einstellungen werden regelmäßig geprüft. Eine Richtlinie zum Ausscheiden von Mitarbeitern (Rechteentzug) sowie eine Passwortrichtlinie sind verabschiedet.
Zugriffskontrolle	Gewährleistung der Benutzung einer DV-Anlage und der gespeicherten Daten entsprechend der Berechtigung	Alle Zugriffsmöglichkeiten und Benutzerrollen sind in Berechtigungskonzepten festgehalten und analog geregelt. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.
Weitergabekontrolle / Übermittlungskontrolle	Gewährleistung der Nachverfolgbarkeit von (gewollten und ungewollten) Datenmanipulationen	Plausibilitätsprüfungen werden durchgeführt.
Auftragskontrolle / Vertragskonformitäts-kontrolle	Sicherstellung der weisungsgemäßen Verarbeitung von Daten im Auftrag	Zum Schutz personenbezogener Daten werden Auftragnehmer hinsichtlich der technischen und organisatorischen Maß-nahmen sorgfältig ausgewählt und entsprechende Auftragsverarbeitungsverträge werden geschlossen. Die technischen und organisatorischen Maßnahmen werden im regelmäßigen Turnus überprüft.
Verfügbarkeitskontrolle	Sicherung von Daten gegen zufällige Zerstörung oder Verlust	Verfügbarkeit, rasche Wiederherstellbarkeit und einen Schutz gegen Verluste werden gewährleistet durch Cloud-Sicherungen. Alle Büros sind mit Feuer- und Rauchmeldeanlagen ausgestattet.
Datentrennungskontrolle / Mandantentrennungs-kontrolle	Sicherstellung der Trennung zu unterschiedlichen Zwecken erhobener Daten	Entwicklungs-/Test- und Produktivumgebung sind voneinander getrennt und Datenverarbeitungssysteme sind zweckgebunden voneinander getrennt. Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind.

Anlage 2
Genehmigte Subunternehmer

Das nachfolgende Unternehmen ist genehmigter Subunternehmer im Sinne der Ziffer 10.1

Firma / Subunternehmen	Anschrift / Land	Leistung
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5, 80807 München, Deutschland	Beratung und technischer Support