WEBSERVICE Steinkampf

Datenschutzvereinbarung nach Artikel 28 der DSGVO und § 62 BDSG (neu) / Vertrag zur Auftragsverarbeitung

© April 2018 eRecht24

Autor: Rechtsanwalt Sören Siebert

www.e-recht24.de

Zwischen den Vertragsparteien

_____

_____

- im Folgenden: Auftraggeber -

und

Heike Steinkampf – Webservice Steinkampf

Ziegeleistr. 5, 31275 Lehrte

- im Folgenden: Auftragnehmer –

wird folgender Vertrag zur Auftragsverarbeitung personenbezogener Daten in Ergänzung der Datenschutzvereinbarung bei Wartung und Systembetreuung des Content-Management-Systems (CMS) sowie der Worldsoft Business Suite (WBS - Customer-Relationship-Managementsystem) und des Vorgänger-Systems OASIS geschlossen:

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis über die Wartung und die Systembetreuung von IT-Systemen.

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG neu), insbesondere des § 62 BDSG (neu) („Auftragsverarbeitung“) geschlossen. Den Parteien ist bekannt, dass ab dem 25.05.2018 die Datenschutz-Grundverordnung (DSGVO - EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsverarbeitung dann grundsätzlich nach Art. 28 DSGVO richten.

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1. Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Betreuungsarbeiten am vom Auftraggeber gemietetem CMS und WBS durch, auf dem dieser personenbezogene Daten speichert. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Systembetreuung der verwendeten IT-Systeme durchzuführen oder durchführen zu können. Der Auftragnehmer wird dadurch zum Auftragsverarbeiter (nach Art. 28 DSGVO). Inhalt des Auftrags, Kategorien

betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.

1.2. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3. Der Zugriff durch den Auftragnehmer auf die Systeme, die zur Verarbeitung der Daten dienen, findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

1.4. Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragnehmers schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

3.5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

3.6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

4. Kontrollbefugnisse des Auftraggebers

4.1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragnehmer wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Im Falle von Maßnahmen der Aufsichtsbehörde verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber i.S.d. Art 58 DSGVO i.V.m. § 40 BDSG (neu) insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme zu gewähren sowie Vorort-Kontrollen zu ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragnehmer dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3. Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren. Einer dem Zweck nach angemessene Vergütung für den entstehenden Aufwand wird genehmigt.

5. Allgemeine Pflichten des Auftragnehmers

5.1. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, auf die er im Zusammenhang mit den Wartungs-/Pflegearbeiten Zugriff erhält, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

5.2. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

5.3. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten bzw. besondere Kategorien personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG bzw. Art. 9 DSGVO oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/EMail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

5.4. Der Datenzugriff außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5. Der Auftragnehmer hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.6. Der Auftragnehmer hat zu gewährleisten, dass sich weitere von ihm beauftragte und befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Fernwartung

6.1. Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

6.2. Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

6.3. Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten oder diese Tätigkeiten ohne seine Anwesenheit durchführt, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

7. Technische und organisatorische Maßnahmen zur Datensicherheit

7.1. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 2** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

7.2. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragnehmer dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

8. Unterstützungspflichten des Auftragnehmers

8.1. Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

8.2. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

9. Einsatz von Unterauftragsnehmern (Subunternehmer)

9.1. Der Auftragnehmer versichert, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

10. Wahrung von Betroffenenrechten sowie Mitteilungspflichten des Auftragnehmers

10.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

10.2. Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsnehmer oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

10.3. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragnehmer erst nach vorheriger Weisung des Auftraggebers durchführen.

10.4. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

10.5. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

11. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Wartung und Betreuung bzw. nach Beendigung dieses Vertrags hat der Auftragsnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsnehmers in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen mit angemessener Fristankündigung vor Ort in Augenschein zu nehmen.

12. Datengeheimnis und Vertraulichkeit

12.1. Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragnehmer bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

12.2. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

12.3. Der Auftragnehmer wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

13. Schlussbestimmungen

13.1. Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

1.1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

1.2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

1.3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

1.4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

_____	Lehrte, den 1. Februar 2020
Ort Datum	Ort Datum
	Hilke Steinkampf
_____	
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst folgende Leistungen:

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Betreuungsarbeiten an den der Worldsoft AG zur Verfügung gestellten Systeme (CMS und WBS/OASIS) durch. Dies umfasst die Erstellung von Formularen, Newslettern und Dokumenten, die zur Erfüllung des Geschäftszweck und -ziel im Rahmen des Online-Marketings und des eCommerce dienlich sind. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Betreuung durchzuführen oder durchführen zu können.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

Adress-Datensätze von Kontakten mit Angaben, soweit über Online-Formulare unter www.domain.com erfasst (Anrede, Vorname, Name, E-Mail-Adresse, Telefon-Nummer sowie themenbezogene Interessen).

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

Interessenten, Kunden, Klienten, Auftraggeber

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

Mit Benutzername und Kennwort geschütztem Zugang über einen Browser auf die bei der Worldsoft AG, Schweiz gespeicherten Server. Der Zugriff erfolgt regelmäßig über ein mit komplexem Passwort geschütztem Computer der Marke Apple, ausgestattet mit Virenschutz, Festplattenverschlüsselung sowie regelmäßiger Änderung der Zugangskennwörter.

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragsverarbeiter zu beachten sind:
[Detaillierte Benennung der einschlägigen Geheimnisschutzregeln; z.B. § 203 StGB]

keine bekannt.

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragnehmers nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

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

✔	Sofern Daten extern gespeichert werden, erfolgt eine physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
✔	Logische Mandantentrennung (softwareseitig)
✔	Berechtigungskonzept
	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
	Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
	Trennung von Produktiv- und Testsystem
Sonstiges:	
✔	Es erfolgt keine lokale Verarbeitung oder Speicherung. Alle Daten sind mandantenbezogen in der Cloud gespeichert und werden serverseitig verarbeitet

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragnehmers:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

Die Volumenverschlüsselung der lokal genutzten Festplatte FileVault (FileVault 2) nutzt die XTS-AES-128-Verschlüsselung mit einem 256-Bit-Schlüssel, um den unautorisierten Zugriff auf die Daten des Startvolume zu verhindern.

2. Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

Es erfolgt keine Pseudonymisierung

3. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (**Zutrittskontrolle**):

Die Verarbeitung der in der Cloud gespeicherten Daten erfolgt ausschließlich über einen Computer mit biometrischer Zugangssperre und / oder Zugang mit Benutzernamen und komplexem Kennwort (keine im Wörterbuch dokumentierte Buchstabenfolge. Dieser Computer befindet sich in einem mit einem manuellem Schließsystem mit Sicherheitsschloss ausgestattetem Büro.
Der Zutritt zum Büroraum erfolgt ausschließlich durch den Auftragsverarbeiter oder das sorgfältig ausgesuchte Reinigungspersonal. Bei Zutritt durch Dritte ist der Auftragsnehmer zugegen. Beim Verlassen des Raums wird das Computersystem gegen unbefugten Zugriff gesperrt.

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (**Zugangskontrolle**):

✔	Zuordnung von Benutzerrechten
✔	Erstellen von Benutzerprofilen
✔	Passwortvergabe
✔	Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
✔	Authentifikation mit biometrischen Verfahren
✔	Authentifikation mit Benutzername / Passwort

✔	Zuordnung von Benutzerprofilen zu IT-Systemen
	Gehäuseverriegelungen
	Einsatz von VPN-Technologie bei der Übertragung von Daten
✔	Verschlüsselung mobiler IT-Systeme
✔	Verschlüsselung mobiler Datenträger
✔	Verschlüsselung der Datensicherungssysteme

	Sperren externer Schnittstellen (USB etc.)
	Sicherheitsschlösser
	Schlüsselregelung (Schlüsselausgabe etc.)
	Personenkontrolle beim Pförtner / Empfang
	Protokollierung der Besucher
✔	Sorgfältige Auswahl von Reinigungspersonal
	Sorgfältige Auswahl von Wachpersonal
	Tragepflicht von Berechtigungsausweisen

✔	Einsatz von Intrusion-Detection-Systemen
✔	Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

✔	Einsatz von Anti-Viren-Software
✔	Verschlüsselung von Datenträgern in Laptops / Notebooks
✔	Einsatz einer Hardware-Firewall
✔	Einsatz einer Software-Firewall:

4. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle):**

✔	Berechtigungskonzept
✔	Verwaltung der Rechte durch Systemadministrator
✔	regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
✔	Anzahl der Administratoren ist das „Notwendigste“ reduziert

✔	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
✔	Sichere Aufbewahrung von Datenträgern

✔	physische Löschung von Datenträgern vor Wiederverwendung
✔	ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
✔	Protokollierung der Vernichtung
✔	Verschlüsselung von Datenträgern

5. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle).**

✔	Protokollierung der Eingabe, Änderung und Löschung von Daten
	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
✔	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.
✔	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts .

6. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle).**

✔	Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
✔	vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
✔	schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)

✔	Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
	Auftragsverarbeiter hat gemäß den gesetzlichen Bestimmungen einen Datenschutz-beauftragten bestellt
✔	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

✔	Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
✔	laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten
✔	Vertragsstrafen bei Verstößen

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (**Transport- bzw. Weitergabekontrolle**):

✔	Einsatz von VPN-Tunneln
✔	Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)

✔	Verschlüsselung physischer Datenträger bei Transport
	Sonstige:

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

	Unterbrechungsfreie Stromversorgung (USV)
	Klimatisierung der Serverräume

	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
	Schutzsteckdosenleisten in Serverräumen

	Feuer- und Rauchmeldeanlagen in Serverräumen
	Feuerlöschgeräte in Serverräumen
	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
	Erstellen eines Backup- & Recoverykonzepts
	Testen von Datenwiederherstellung

	Erstellen eines Notfallplans
	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
	Serverräume nicht unter sanitären Anlagen
	In Hochwassergebieten: Serverräume über der Wassergrenze
	belastbares Datensicherungs- und Widerherstellungskonzept vorhanden

Sonstige: da keine lokale Speicherung der Daten erfolgt, sondern direkt über einen Internetzugriff auf die Systeme des Hosters Worldsoft AG zugegriffen wird, sind vorstehende Maßnahmen unter III. nichtzutreffend bzw. obliegen dem Hoster. Ein separater Vertrag zur Auftragsverarbeitung wurde mit der Worldsoft AG geschlossen.

IV. **Besondere Datenschutzmaßnahmen**

Es liegen schriftlich vor:

	interne Verhaltensregeln
	Risikoanalyse
	Datenschutz-Folgenabschätzung

	Datensicherheitskonzept
	Wiederanlaufkonzept Zertifikat:

Sonstige: da keine lokale Speicherung der Daten erfolgt, sondern direkt über einen Internetzugriff auf die Systeme des Hosters Worldsoft AG zugegriffen wird, sind vorstehende Maßnahmen unter III. nichtzutreffend bzw. obliegen dem Hoster. Ein separater Vertrag zur Auftragsverarbeitung wurde mit der Worldsoft AG geschlossen.

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von zwölf Monaten / Jahren und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Ort der Leistungserbringung
Keine Subunternehmer vorhanden		