Datenschutzvereinbarung
Wartung und Pflege von IT-Systemen

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

zwischen

Holzwarth

Goethestr. 10

71332 Waiblingen

- Auftraggeber -

und

hz Soft- und Hardware GmbH

Erwin-Bahnmüller-Str. 31

71394 Kernen

- Auftragnehmer -

Präambel

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

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG), insbesondere des § 11 BDSG („Auftragsdatenverarbeitung“) 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 Auftragsdatenverarbeitung dann grundsätzlich nach Art. 28 DSGVO richten.

1. Allgemeines

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. 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 Pflege von IT-Systemen durchzuführen oder durchführen zu können.

2. Dauer und Beendigung des Auftrags

(1) Der Auftragnehmer führt für den Auftraggeber Leistungen (Wartung und/oder Pflege von IT-Systemen) durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag“), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z.B. BGB) basiert. Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

3. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Prüfung und Wartung der IT-Infrastruktur (Server, Clients, Drucker, Netzwerkswitche, Firewall, Telekommunikationsgeräte)
- Prüfung, Installation und Wartung von Betriebssystemen und Softwareprogrammen
- Fehleranalysen, Installationen und Wartungen können auch per Fernwartung erfolgen

Hierbei ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/Datenarten hat:

- Nutzungsdaten
- Bestandsdaten

Kreis der von der Datenverarbeitung Betroffenen:

- Kunden, Lieferanten, Interessenten des Auftraggebers
- Mitarbeiter

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können

☒ schriftlich
☒ per Fax
☒ per E-Mail
☒ mündlich

erfolgen.

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

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

5. Allgemeine Pflichten des Auftragnehmers

(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.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(3) 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.

(4) 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/E-Mail) 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) Der Auftragnehmer wird ab dem 25.5.2018 seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

6. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. § 38 BDSG bzw. ab dem 25.05.2018 nach Art. 58 DSGVO i.V.m. § 40 BDSG (neu), insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

7. Fernwartung

(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.

(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.

(3) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

8. Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.

(2) Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach § 9 BDSG bzw. ab dem 25.05.2018 nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bzw. ab dem 25.05.2018 nach Art. 37 DSGVO i.V.m. § 38 BDSG (neu) bestellt hat, soweit dieser gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9. Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG bzw. ab dem 25.05.2018 zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet wurden. Ab dem 25.5.2018 wird der Auftragnehmer stattdessen die in Satz 2 genannten Personen in einer dem Art. 28 Abs. 3 lit. b) genügenden Weise zur Vertraulichkeit verpflichten, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Wahrung von Betroffenenrechten

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

(2) Für den Fall, dass der Auftragnehmer die Wartung und Pflege von IT-Systemen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt (z.B. auch im Falle der Fernwartung), sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG als **ANLAGE** zu diesem Vertrag zu dokumentieren. Ab dem 25.05.2018 hat der Auftragnehmer eine Beschreibung der von ihm getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO dem Auftraggeber in geeigneter Weise zur Verfügung zu stellen. Dies beinhaltet auf Aufforderung des Auftraggebers auch Nachweise über das nach Art. 32 Abs. 1

lit. d) einzurichtende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

12. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

13. Schlussbestimmungen

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

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

WN , den 17.5.18	Kernen , den 02.05.2018
Ort Datum	Ort Datum
- Auftraggeber -	- Auftragnehmer -

ORTHOPÄDIE
HOLZWARTH
SCHUHTECHNIK
INHABER HARALD RUML
Goethestraße 10 · 71332 Waiblingen
Tel. 07151 51495 · Fax 07151 563223

ANLAGE 1

Beschreibung der ergriffenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit gem. Art. 32 EU-DSGVO.

1. Maßnahmen zur Zutrittskontrolle

Maßnahmen	**Beschreibung**
Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)	Es besteht eine klare Regelung zu befugten Personen. Der Zutritt erfolgt berechtigungsspezifisch. Der Zutritt zum Unternehmensgebäude erfolgt per (persönlicher) Zutrittskarte. Innerhalb des Gebäudes ist der Zutritt zu Bereichen mit erhöhtem Sicherheitsbedarf (IT-Administration) zusätzlich über Schließsysteme gesichert. Die Vergabe von Zutrittsberechtigungen erfolgt ausschließlich unter Berücksichtigung der Aufgabenbereiche der Mitarbeiter.
Besucherregelung	Besucher müssen sich beim Empfang anmelden. Es erfolgt eine Abholung am Empfang. Besucher werden stets durch Mitarbeiter auf dem Betriebsgelände begleitet. Die Begleitung erfolgt nach dem Besuch bis zum Ausgang.
Schlüsselregelung	Sämtliche Zugangskarten sind in einer tagesaktuellen Schlüsselliste dokumentiert.
Sicherung der Gebäude und des Unternehmensgeländes	Das Gebäude ist auch außerhalb der Arbeitszeit durch Videoüberwachung und Maßnahmen zum Einbruchsschutz gesichert.

2. Maßnahmen zur Zugangskontrolle

Maßnahmen	**Beschreibung**
Antrag zur Vergabe von Benutzer-Accounts	Die Freigabe zur Einrichtung bzw. Anpassung von Benutzerkonten geschieht nach Durchlauf eines Prüfungs- und Genehmigungsprozesses.
Absicherung der DV-Systeme durch Login-Prozedur	Der Zugang ist passwortgeschützt und die Zugangsdaten nur ausgewählten Mitarbeitern bekannt.
Passwortrichtlinie (bzgl. Länge, Änderungsintervall, etc.)	mindestens 8 Zeichen Groß-/Kleinschreibung, Zahlen, Sonderzeichen 3 der 4 Kriterien müssen erfüllt sein Richtlinien und Vorgaben für die Passwortsicherheit sind vorhanden und werden automatisch geprüft.
Sicherungsmaßnahmen bei Verlassen des Arbeitsplatzes	Beim Verlassen des Arbeitsplatzes wird der Rechner vom Benutzer gesperrt. Bei Dienstschluss werden die Mitarbeiter-PCs heruntergefahren. Eine automatische Abschaltung oder ein Zugangsschutz durch Bildschirmschoner bei Inaktivität ist nicht unternehmensweit eingerichtet.

	Die Mitarbeiter sind jedoch hinsichtlich der Sperrung ihrer Arbeitsplätze beim Verlassen sensibilisiert.
Passwortsperrung nach mehrmaligen Fehlversuchen	Fehlgeschlagene Anmeldungen werden protokolliert. Mitarbeiter-PCs werden nach mehrmaliger Falscheingabe des Passwortes automatisch gesperrt. Die Sperre erfolgt, wenn innerhalb von 2 Minuten 5 falsche Eingaben erfolgen.
Regelungen / Voraussetzungen zur Telearbeit	Innerhalb des Auftragsverhältnisses erfolgt die Einrichtung von Telearbeitsplätzen nur mit Zustimmung des Auftraggebers.
Absicherung der Netzwerkverbindung bei Telearbeit (z.B. VPN, Zugangstoken)	Soweit Telearbeitsplätze mit Zustimmung des Auftraggebers eingerichtet werden, wird der Zugang durch eine SSLVPN-Verbindung oder Direct Access gesichert.
Einrichtung eines Benutzerstammsatzes pro User (keine Gruppen-Accounts)	Alle Personen / Mitarbeiter erhalten ihr eigenes Benutzerkonto.
Verwahrung von Daten und Dokumenten	Digitale Daten befinden sich auf gesicherten Systemen. Nicht digitale Daten/Dokumente lagern in verschlossenen Schränken / Behältnissen. Aus dem Produktionsprozess herausgelöste Datenträger werden durch zertifizierte Entsorgungsunternehmen datenschutzgerecht entsorgt. Backups werden nicht auf mobile Datenträger (Bänder o.ä.) gezogen. Der Einsatz von USB-Speichern ist nur den Mitarbeitern aus der IT-Administration gestattet. Der Verlust mobiler Geräte (z.B. durch Aufbruch eines Service-Wagens) ist unverzüglich anzuzeigen. Diese Geräte werden für den Zugang zu internen Netzen unverzüglich gesperrt.

3. Maßnahmen zur Zugriffkontrolle

Maßnahmen	**Beschreibung**
Zentrale Vergabestelle von Benutzerrechten	Die Vergabe von Rechten erfolgt sowohl für Kunden, als auch Mitarbeiter über zentrale Systeme.
Formales Antrags- und Genehmigungsverfahren	Der Umfang der Berechtigungen ist abhängig von der Arbeitsplatz-/Tätigkeitsbeschreibung des Mitarbeiters. Mitarbeiter können selbständig keine Rechte anfordern und einrichten. Die Erweiterung von Rechten ist stets durch den Abteilungsleiter bei der IT-Administration schriftlich anzufordern. Bei Ausscheiden eines Mitarbeiters wird die IT-Administration unverzüglich durch die Personalabteilung informiert. Zum Ausscheidungszeitpunkt werden die Berechtigungen aufgehoben und ggf. eingerichtete Zugänge gelöscht.
Regelung der Zugriffsberechtigung auf Basis definierter Rollen, nicht personengebunden	Der Zugriff auf verschiedene Dienste bzw. Systeme ist durch Gruppenrichtlinien geregelt. Diese werden zentral gesteuert. Ausgangspunkt ist die Arbeitsplatzbeschreibung des Mitarbeiters. Ausschließlich erforderliche Rechte werden über den Abteilungsleiter bei der IT-Administration angefordert.

Ständige Aktualisierung der Zugriffsrechte sowie anlassbezogene Anpassung z.B. beim Abteilungswechsel eines Mitarbeiters innerhalb der Organisation	Es ist organisatorisch geregelt, dass die Rechte der Mitarbeiter bei Änderung ihrer Zuständigkeiten entsprechend angepasst werden.
Zeitliche Begrenzung der Zugriffsmöglichkeiten	Mitarbeiter erhalten nur solange Zugriff auf die entsprechenden Daten, wie dieser für die jeweiligen Aufgaben benötigt wird.
Richtlinien für die Dateiorganisation	Es existieren Vorgaben zur Ablage bzw. Speicherung der Daten bzw. Information durch Mitarbeiter. Die Mitarbeiter nutzen im Rahmen der ihnen eingeräumten Berechtigungen ausschließlich zur Nutzung durch die Unternehmensleitung freigegebene Software. Die Datenspeicherung innerhalb der eingesetzten Software wird durch die Datenbankstruktur und die eingeräumten Rechte bestimmt. Laufwerksfreigaben/Ordnerfreigaben werden nur auf Anforderung durch Abteilungsleiter eingerichtet. Auf Daten im Intranet haben nur die Mitarbeiter einen schreibenden Zugriff, die zur Datenpflege legitimiert sind. Alle Mitarbeiter sind für ihre Arbeitsbereiche hinsichtlich der eingesetzten Software und den vorhandenen Speichermöglichkeiten unterrichtet/geschult.
Firewall	Alle Systeme und Netzabschnitte sind durchgehend durch redundante Firewallsysteme geschützt.

4. Maßnahmen zur Weitergabekontrolle

Maßnahmen	**Beschreibung**
Verschlüsselung bei der Datenübermittlung	Datenübertragungen können verschlüsselt erfolgen.
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger und Informationen	Datenträger werden physisch zerstört. Die Löschung von Daten erfolgt nach Ablauf der gesetzlichen oder vertraglichen Nachweis- und Aufbewahrungspflichten. Die datenschutzgerechte Vernichtung wird durch den Datenschutzbeauftragten sichergestellt.
Dokumentation der Abruf- und Übermittlungsprogramme	Die eingesetzten Programme sind alle sowohl für die Mitarbeiter, als auch Kunden dokumentiert.
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der genutzten Übermittlungswege (Konfiguration)	Alle Übermittlungsverfahren sind dokumentiert. Mobile Datenträger werden nicht eingesetzt. Kuriere kommen deshalb nicht zum Einsatz.
Bestimmte autorisierte Benutzer	Es gibt autorisierte Benutzer für verschiedene Arbeitsbereiche, welche spezielle Rechte in Hinsicht auf personenbezogene Daten haben, da diese für die normale Arbeit oder die Fehlersuche benötigt werden.
Fernwartungskonzept	Art, Umfang und Befugnisse für die Fernwartung sind dokumentiert und werden über Managementtools umgesetzt.

	Der Zugriff auf die Systeme des Auftraggebers kann Webbasiert erfolgen. Dies gilt für Auftragnehmer und Auftraggeber gleichermaßen. Auf Wunsch kann der Zugriff durch den Auftragnehmer stets telefonisch angekündigt/genehmigt werden.

5. Maßnahmen zur Eingabekontrolle

Maßnahmen	**Beschreibung**
Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe	Die Berechtigung für die Eingabe/Verarbeitung von Daten durch zuständige Personen ist geregelt.
Verfahrens-, Programm- und Arbeitsablauforganisation	Für alle relevanten Tätigkeiten gibt es grundlegende Dokumentationen.
Authentizität	Bei Bedarf kann über entsprechende Logs eingesehen werden, wann welcher Nutzer Daten angelegt, bearbeitet oder gelöscht hat. Die Identifizierung der Nutzer wird durch die Authentifizierung bei der Anmeldung sichergestellt.
Revisionsfähigkeit	Durch die Standardfunktion „Journal“ kann nachvollzogen werden, wer wann welche Daten verändert hat.
Transparenz	Durch die Standardfunktion „Journal“ kann nachvollzogen werden, wer wann welche Daten verändert hat.

6. Maßnahmen zur Auftragskontrolle

Maßnahmen	**Beschreibung**
Auswahl der (Unter-)Auftragnehmer	Die Auswahl der Auftragnehmer erfolgt unter sorgfältiger Prüfung dessen datenschutzrechtlicher Zuverlässigkeit. Die Prüfung der durch einen Unterauftragnehmer ergriffenen Maßnahmen auf ihre datenschutzrechtliche Geeignetheit erfolgt durch den Datenschutzbeauftragten des Auftragnehmers.
Regelmäßige Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben beim Auftragnehmer	Eine Kontrolle durch den Auftraggeber (z.B. per Begehung durch einen Sachverständigen) ist nach vorheriger Anmeldung jederzeit möglich. Im konkreten Fall erfolgt mangels Unterbeauftragung keine Kontrolle von Unterauftragnehmern.

7. Maßnahmen zur Verfügbarkeitskontrolle

Maßnahmen	**Beschreibung**

Backup	Es existiert ein aktuelles Backupkonzept für das Rechenzentrum der Auftragnehmerin.
	Das Backup erfolgt als Disaster Recovery-Backup.
	Alle VMs werden einmal täglich gesichert. Diese Sicherung wird 7 Tage aufbewahrt. Die Sicherung der VMs ist unabhängig von den Anwendungen, die innerhalb der VM laufen. Die Wiederherstellung aus dieser Sicherung erfolgt immer als vollständige VM.
Reaktionen im Notfall	Es existiert ein aktuelles Notfallkonzept für das Rechenzentrum der Auftragnehmerin. Das Notfallkonzept beinhaltet die Information des Datenschutzbeauftragten. Im weiteren Verlauf stellt der Datenschutzbeauftragte im Rahmen seiner Verantwortlichkeit und unter Berücksichtigung der gesetzlichen Anforderungen die Information des Auftraggebers und ggf. der Aufsichtsbörden mit Zustimmung des Auftraggebers sicher.
Absicherungen im Rechenzentrum	– Elektronische und mechanische Zugangskontrollsysteme – Videoüberwachung vor dem Gebäudekomplex und auf dem Gelände – Brandbekämpfungseinrichtungen – Klimatisierung über getrennte Kühlkreisläufe – redundante Stromzuführung – unterbrechungsfreie und gefilterte Stromversorgung durch USV-Batterien (Online USV)
Internetanbindungen	– Zweifach-redundante IP-Anbindung des Datacenter
Patchmanagement	Das Patchmanagement der Umgebung erfolgt regelmäßig in Abhängigkeit der von Microsoft bereitgestellten Patches und Fixes. Die Auftragnehmerin behält sich vor, einzelne Patche oder größere Servicepacks erst mit angemessener Verzögerung zu installieren, um ggfs. Erfahrungswerte im Hinblick auf die Systemstabilität zu sammeln.
Virenschutz	Zentrale Komponenten, sowie auch alle Mitarbeitersysteme werden vor Viren geschützt. Ein Virenschutzkonzept ist als Bestandteil des Betriebshandbuchs vorhanden und umgesetzt.
Firewall	Zentrale Komponenten, sowie auch alle Mitarbeitersysteme werden vor Angriffen von außen geschützt. Ein Firewallkonzept ist als Bestandteil des Betriebshandbuchs vorhanden und umgesetzt.

8. Maßnahmen zum Trennungsgebot

Maßnahmen	**Beschreibung**
Mandantentrennung	Werden Daten der Auftraggeberin auf den Systemen der Auftragnehmerin gespeichert, werden diese logisch getrennt verarbeitet.
Funktionstrennungen	Die Funktionstrennung gemäß Art. 5 Abs. 2 ist gegeben. Die verschiedenen organisatorischen Bereiche der Auftragnehmerin (wie Entwicklung und Support) erhalten nur Zugriff auf die für ihre Aufgaben relevanten Daten.