

RAHMENVERTRAG | VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Für die Auftragsdatenverarbeitung gemäß BDSG bzw. DSGVO

Die Vertragsparteien

AUFTRAGGEBER	AUFTRAGNEHMER
Firmenbezeichnung	WEB9 Prakrong & Torsten Zimmermann GbR Firmenbezeichnung
Geschäftsführer / Inhaber	Torsten Zimmermann Geschäftsführer / Inhaber
Straße und Hausnummer	Alte Bundesstraße 17 Straße und Hausnummer
PLZ und Ort	D-76689 Karlsdorf-Neuthard PLZ und Ort

schließen folgenden Vertrag:

§1 Allgemeine Bestimmungen und Auftragsgegenstand

- 1.1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (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. Die Verarbeitung der Daten durch den Auftragnehmer 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 S der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.
- 1.4. Die Vergütung wird außerhalb dieses Vertrags vereinbart.

§2 Vertragslaufzeit und Kündigung

- 2.1. 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 gegenüber 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 zu 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 Weisungen 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.

§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 im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme / -systeme gewähren sowie Vorort-Kontrollen ermöglichen.
- 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 Vorlaufzeit 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.

§5 Allgemeine Pflichten des Auftragnehmers

- 5.1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedstaatlicher Rechtsvorschriften zulässig (z.B. in Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 5.2. Der Auftragnehmer hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.
- 5.3. Sofern der Auftragnehmer nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen im Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert den Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.
- 5.4. Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten 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.
- 5.5. Der Auftragnehmer wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

§6 Technische und Organisatorische Maßnahmen

- 6.1. 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.
- 6.2. 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.

§7 Unterstützungspflichten des Auftragnehmers

- 7.1. Der Auftragnehmer wird den Auftraggeber gemäß 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.

- 7.2. Der Auftragnehmer wird dem 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 Auftragnehmer zur Verfügung stehenden Informationen.

§8 Einsatz von Subunternehmern

- 8.1. Der Auftragnehmer ist nur mit Zustimmung des Auftraggebers zum Einsatz von Subunternehmern berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 beigelegt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies den Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.
- 8.2. Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- / Transportdienstleistung, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.
- 8.3. Wesentliche Verträge zwischen Auftragnehmer und Subunternehmer müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und im vollen Umfang auch gegenüber dem Subunternehmer ausgeübt werden können. Der Auftragnehmer ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragnehmers einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.
- 8.4. Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber gegenüber dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie gegenüber dem Auftragnehmer berechtigt ist. Der Auftragnehmer hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragnehmer vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.
- 8.5. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn dieser seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO gegenüber den ihm unterstellten Personen erfüllt hat.
- 8.6. Der Auftragnehmer ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Subunternehmer verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
- 8.7. Der Auftragnehmer hat sich von seinen Subunternehmern bestätigen zu lassen, dass diese - soweit gesetzlich vorgeschrieben - einen Datenschutzbeauftragten benannt haben.
- 8.8. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen nach Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

§9 Mitteilungspflichten des Auftragnehmers

- 9.1. 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 Subunternehmer oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.
- 9.2. Der Auftragnehmer ist verpflichtet, dem 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.
- 9.3. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.
- 9.4. Der Auftragnehmer 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 Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

§10 Vertragsbeendigung, Löschung und Rückgabe der Daten

- 10.1. Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer 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 Auftragnehmers in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

§11 Datengeheimnis und Vertraulichkeit

- 11.1. 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.
- 11.2. 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 Auftragnehmer aufnehmen.
- 11.3. Der Auftragnehmer wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

§12 Schlussbestimmungen

- 12.1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form. Änderungen zur betreffenden Vertragsvorversion sind deutlich zu kennzeichnen.
- 12.2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, so gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.
- 12.3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, so bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
- 12.4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.
- 12.5. Mit Unterzeichnung dieses Vertrags kennen beide Parteien dessen Bestimmungen an und bestätigen, dass sie in Bezug auf das betreffende Unternehmen unterschriftsberechtigt sind.

.....
Ort, Datum

.....
Ort, Datum

.....
Auftraggeber

.....
Auftragnehmer, WEB9

ANLAGE 1

Der vorliegende Vertrag umfasst folgende Leistungen:

- Erstellung von Printmaterialien mit personenbezogenen Inhalten (Visitenkarten, etc.)
- Erstellung, Hosting, Wartung, Konfiguration, Migration und Bearbeitung von Webanwendungen sowie Apps und somit Datei- und Datenbank-Inhalten inklusive Benutzerdaten und Kundeninformationen (Beispielsweise bei Webshops oder bei Funktionen in sozialen Medien)
- Hosting und Betrieb von Mailservern und somit Mailkonten und Weiterleitungen
- Tracking (auch Server-Logs) von Websitebesuchern zur anonymisierten statistischen Verarbeitung und zum Schutz vor Angriffen
- Unterstützung und Konzeption von Marketingmaßnahmen (Beispielsweise Erstellung von Newslettern oder Nachrichten)

Im Rahmen der Leistungserbringung werden regelmäßig folgende Daten verarbeitet:

- Personendaten (z.B. Namen, Geburtsdaten, Anschrift)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsdaten (z.B. Zahlungsdaten, Zahlungsmittel)
- Protokolldaten (z.B. IP-Adresse)

Bei dem Kreis der Personen, welche die Daten verarbeiten, handelt es sich um:

- der Auftraggeber und dessen Mitarbeiter
- sowie Kunden oder Interessenten des Auftraggebers (z.B. bei Newslettern, Medien-Kanäle und Webshops)

Der Zugriff auf die Daten geschieht in folgender Weise:

- Die Daten werden entweder von Kunden oder Interessenten des Auftraggebers über einer Webanwendung (Formular / Anmeldung / Shop) eingetragen. Diese Daten werden, je nach Einsatzzweck, in einer Datenbank gespeichert oder nur kurzfristig verarbeitet und an den Auftraggeber per E-Mail versendet. Diese Verarbeitung ist innerhalb der Browser mit einer SSL verschlüsselten Verbindung geschützt. Für die Nutzung des verschlüsselten E-Mail-servers bei Abruf der Daten per E-Mail ist der Auftraggeber verantwortlich.
- Von Auftragsverarbeiter zu Wartungs- und Konfigurationszwecken über verschlüsselte SSL oder SSH Verbindungen, zusätzlich geschützt über Benutzer/Passwort-Authentifizierung.

Folgende Geheimnisschutzregeln sind von Auftraggeber und -nehmer zu beachten:

- Detaillierte Benennung der einschlägigen Geheimnisschutzregeln; z.B. §203 StGB

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 in Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

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

- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Die im Auftrag verarbeiteten Passwörter werden mit gängigen Verschlüsselungstechnologien verschlüsselt.

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

- Absicherung von Gebäudeschächten
- Chipkarten-Schließsystem oder manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Kontrolle der Besucher
- Sorgfältige Auswahl von Reinigungspersonal

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

- Zuordnung von Benutzerrechten

- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- Authentifikation mit Benutzername / Passwort
- Verschlüsselung der Datensicherungssysteme (bei Backups und Passwörtern)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Kontrolle der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

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:

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. beim Ausscheiden von Mitarbeitern o. ä.)
- Anzahl der Administratoren ist auf das Notwendigste reduziert
- Passworrichtlinie inkl. Passwortlänge, Passwortwechsel
- sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
- Weitergabe ausschließlich über digitalen Zugriff mit passwortgeschützter Zugriffskontrolle

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

- Dauerhaft aktiver DDoS-Schutz
- Klimatisierung der Serverräume
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage
- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages
- Einsatz einer Softwarefirewall
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- belastbares Datensicherungs- und Wiederherstellungskonzept vorhanden
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Der Auftragnehmer wird, die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 24 Monaten und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

ANLAGE 3

Liste der aktuell bestehenden Subunternehmer

Produkt / Dienstleistung	Subunternehmer
Rechenzentrum (Standard) Verfügbarkeit 99,9%	Hetzner Online Datacenterpark Sigmundstraße 135 99431 Nürnberg, Germany Hetzner Online Datacenterpark Am Datacenterpark I 98223 Falkenstein, Germany
Rechenzentrum nach DIN 27000 Verfügbarkeit 99,998%	WEB9 RZ München, eine Division der WEB9
Analysewerkzeuge	StatCounter Guinness Enterprise Centre Taylor's Lane Dublin 8. Ireland
Analysewerkzeuge, Tools, Online-Kartensystem und Web-Fonts	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043, USA
Online-Kartensystem	OpenStreetMap Foundation 132 Maney Hill Road Sutton Coldfield West Midlands, B72 1JU, UK