Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen

_____

Firma, Straße, Hausnummer, Postleitzahl, Ort

_____

Kundennummer

- nachstehend Auftraggeber genannt -

und

SPIEGLHOF media GmbH, Luitpoldstraße 4, 84034 Landshut

- nachstehend Auftragnehmer genannt -

1. Allgemeine Bestimmungen und Auftragsgegenstand

1. Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag mit den Leistungen:
(bitte entsprechend ankreuzen)

☐ 1. Managed Server: Nutzung eines dedizierten Serversystems durch den Auftraggeber, Pflege, Management des dedizierten Serversystems durch den Auftragnehmer

☐ 2. Webhosting: Nutzung eines Speicherplatzes (Webspace) auf einem Internetserver durch den Auftraggeber. Nutzung eines E-Mailservers (Empfangen, Versenden und Speichern von E-Mails) durch den Auftraggeber. Technische Betreuung des Speicherplatzes und E-Mailservers durch den Auftragnehmer

☐ 3. Domains: Nutzung eines Domainverwaltungssystems auf einem Internetserver durch den Auftraggeber. Anwendungsbetreuung des Domainverwaltungssystems durch den Auftragnehmer. Beauftragung der Registrierung von SSL-Zertifikaten durch den Auftragnehmer.

☐ 4. Webentwicklung: Entwicklung, Updates von Webanwendungen des Auftraggebers durch den Auftragnehmer.

Bei Leistung Managed Server:
Der Hauptvertrag beinhaltet keine Miete eines physischen Servers mit Besitzübergang. Der Auftraggeber hat keine vor-Ort-Zugangsberechtigung zum Server. Der Hauptvertrag hat primär nicht die Verarbeitung personenbezogener Daten durch den Auftragnehmer zum Gegenstand. Dass der Auftragnehmer im Rahmen der Leistungserbringung mit personenbezogenen Daten in Kontakt kommt, kann jedoch nicht ausgeschlossen werden. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag ergeben. Im Übrigen wird der Hauptvertrag durch diese Vereinbarung nicht berührt. Sofern in dieser Vereinbarung lediglich von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO.

Bei Leistung Domains und SSL-Zertifikate:
Im Rahmen der Registrierung von Domain-Namen oder der Beantragung von SSL-Zertifikaten ist es für die Vertragserfüllung zwingend erforderlich, u.a. personenbezogene Daten an die jeweilige Registrierungsstelle (im Folgenden: „Registry“) bzw. Zertifizierungsstelle (sog. Certifcate Authority, im Folgenden: „CA“) zu übermitteln, um den jeweiligen Auftrag auszuführen. So kommen bei Domainregistrierungen teilweise (z.B. bei der Registrierung von .de-Domains mit der Denic eG), bei Zertifikatsbestellungen stets direkte Verträge zwischen dem Lieferanten (Registry bzw. CA) und dem jeweiligen Inhaber zustande. In diesem Zusammenhang kann es (in Abhängigkeit von der jeweils zuständigen Registry bzw. CA) vorkommen, dass eine Übermittlung personenbezogener Daten in Drittstaaten, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, stattfndet (z.B. bei der Beauftragung zur Registrierung einer .com-Domain). Teilweise sind die übermittelten Daten über Datenbanken (sog. WHOIS-Datenbanken), bzw. bei SSL-Zertifikaten über bestimmte Browserfunktionen, öffentlich einsehbar teilweise werden Daten auch an das RIPE NCC in den Niederlanden weitergeleitet, das ebenfalls eine öffentliche Datenbank im Internet unterhält. Schließlich werden bei einer Registrierung von Domains unterhalb einer generischen Top Level Domain (sog. gTLDs, wie z.B. .com, .net, .org, .biz etc.) u.a. die Inhaberdaten an die Internet Corporation for Assigned Names and Numbers (ICANN), Los Angeles, USA, weitergeleitet. Bei Registrierung von SSL-Zertifikaten werden Daten an die Sectigo Limited Headquarters, 5 Becker Farm Road, Roseland, NJ 07068, United States weitergeleitet. Die genannten Datenübermittlungen sind für Domainregistrierungen bzw. Bestellungen von SSL-Zertifikaten, mithin für die Vertragserfüllung, zwingend erforderlich. Soweit er für Dritte Domains registriert oder SSL-Zertifikate bestellt, garantiert der Auftraggeber ausdrücklich die Rechtmäßigkeit der Verarbeitung i.S.d. Art. 6 DSGVO. Gleiches gilt, sofern er bei den Domainkontakten personenbezogene Daten von Mitarbeitern einträgt.

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.
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 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

2. Vertragslaufzeit und Kündigung

1. Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses beendet gleichzeitig diese Vereinbarung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

3. Weisungen des Auftraggebers

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 leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.
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. 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.
4. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

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. 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. 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.

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.
3. Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeinte Pflichten des Auftragnehmers

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. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im 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.
2. 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.
3. Sofern der Auftragnehmer nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Die Kontaktdaten des Datenschutzbeauftragten sind auf https://spieglhof-media.de abrufbar.
4. Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragnehmers oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice der Mitarbeiter des Auftragnehmers) ist gestattet.
5. 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.
6. Der Auftragnehmer wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

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.
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

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.
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 Auftragnehmer zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragnehmern

1. Der Auftragnehmer ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragnehmern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 2 beigefügt. Für die in Anlage 2 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem 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.
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- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit 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.

3. Sämtliche Verträge zwischen Auftragnehmer und Unterauftragnehmer (Subunternehmerverträge) 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 in vollem Umfang auch gegenüber dem Unterauftragnehmer 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.
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 ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. 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.
5. Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO gegenüber den ihm unterstellten Personen erfüllt hat.
6. Der Auftragnehmer ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragnehmer verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
7. Der Auftragnehmer ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragnehmer verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
8. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilung des Auftragnehmers

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 Unterauftragnehmer oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

2. 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.
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.
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

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).

11. Datengeheimnis und Vertraulichkeit

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

SPIEGLHOF media

12. Schlussbestimmungen

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.
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.
3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.
4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.
5. Es gilt das Recht der Bundesrepublik Deutschland.
6. Die Parteien vereinbaren als Gerichtsstand den Sitz des für Landshut zuständigen Gerichts.
7. Dieser Vertrag wird mit einer Versionsnummer – auf jeder Seite am Ende ersichtlich - gekennzeichnet. Bei Änderungen, Korrekturen, Erweiterungen des Vertrages erhöht sich die Versionsnummer. Dem Auftraggeber wird per E-Mail der Vorgang mitgeteilt. Eine erneute schriftliche Unterzeichnung ist nicht erforderlich. Das Recht auf Widerspruch bleibt davon unberührt. Die Änderungen werden in einem Changelog protokolliert.

_____ _____

Ort, Datum Unterschrift Auftraggeber

Landshut, den 29.11.2019
Ort, Datum

Unterschrift Verfügungsberechtigter

Anlage 1 - Auftragsdetails

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- Personendaten (Adressdaten)
- E-Mailadressen
- IP-Adressen, die im Rahmen von Logs automatisiert gespeichert und verarbeitet werden
- Cookies, die im Rahmen von betriebenen Webseiten automatisiert gespeichert und verarbeitet werden

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:
(bitte entsprechend ankreuzen oder fehlende Personen ergänzen)

- ☐ Beschäftigte
- ☐ Kunden
- ☐ Abonnenten
- ☐ Interessenten
- ☐ Geschäftspartner
- ☐ Lieferanten
- ☐ Dienstleister
- ☐ Bewerber
- ☐ _____

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

- per Webseitenaufruf über eine ausschließlich verschlüsselte Verbindung
- per Direktzugriff (Shell/Konsolenzugriff) über eine ausschließlich verschlüsselte Verbindung

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragnehmer zu beachten sind:

_____

_____

_____

Anlage 2 - Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragnehmers

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um:

I. Vertraulichkeit

Zutrittskontrolle

Auftraggeber und Auftragnehmer haben keinen physischen Zugang zum Leistungsgegenstand des Hauptvertrags

Zugangskontrolle

Account-Passwörter, welche vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind.

Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

Rootzugriff besteht nur für berechtigte Mitarbeiter des Auftragnehmers. Der administrative SSH-Zugriff erfolgt ausschließlich über Public/-Private-Key Authentifizierung.

Zugriffskontrolle

Bei Verwaltungssystemen des Auftragnehmers wird durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) sichergestellt, dass unberechtigte Zugriffe verhindert werden.

Für installierte Daten/Software durch den Auftragnehmer ist einzig dieser in Bezug auf Sicherheit und Updates zuständig.

Für installierte Daten/Software durch den Auftraggeber ist einzig dieser in Bezug auf Sicherheit und Updates zuständig.

Datenträgerkontrolle

Festplatten werden nach Beendigung des Hauptvertrags mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.

Trennungskontrolle

Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.

Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung

Wo möglich und technisch sinnvoll, werden personenbezogene Daten pseudonymisiert. Für die Umsetzung ist der Auftraggeber zuständig.

Anonymisierung

Dem Auftraggeber steht für die Anonymisierung von IP-Adressen eine Funktion im Verwaltungstool zur Verfügung. Für die Aktivierung ist der Auftraggeber zuständig.

II. Integrität

Weitergabekontrolle

Alle Mitarbeiter sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

Es erfolgt eine datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungserbringung des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

Änderungen personenbezogener Daten durch den Auftragnehmer werden in einem Ticketsystem protokolliert und können nachträglich abgerufen werden. Der Auftragnehmer nimmt grundsätzlich keine mündlich erteilten Aufträge an.

Bei Änderungen personenbezogener Daten durch den Auftraggeber obliegt die Verantwortung der Eingabekontrolle beim Auftraggeber.

III. Verfügbarkeit und Belastbarkeit

Werden gewährleistet durch

Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.

Einsatz von Festplattenspiegelung.

Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage seitens des Rechenzentrums

Einsatz von Softwarefirewall und Portreglementierungen.

DDoS-Schutz seitens des Rechenzentrums

Monitoring der Serverdienste

Einsatz von Viren- und Spamfiltern

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

Das Datenschutzmanagement hat das Ziel, die Eintrittswahrscheinlichkeit für Datenpannen oder Datenschutzverstöße zu verringern und im Falle eines Eintritts den Schaden und das Risiko für die betroffenen Personen zu begrenzen. Dies wird durch den Auftragnehmer nach dem PDCA-Prinzip erarbeitet und ausgeführt.

Datenschutzfreundliche Voreinstellungen

Bei der Entwicklung oder Änderung eines Produkts für die Leistungserbringung des Hauptauftrages wird darauf geachtet, dass ausschließlich diejenigen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Gleiches gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Auftragskontrolle

Mitarbeiter des Auftragnehmers werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Eine Auftragskontrolle beim Auftragnehmer erfolgt, soweit dies für die Auftragsdurchführung erforderlich ist.

Anlage 3 - Liste der bestehenden Subunternehmer

Zum Zeitpunkt des Vertragsschlusses setzt der Auftragnehmer keine Subunternehmer ein.

Anlage 4 - Changelog

Version	Datum	Beschreibung
1.0	22.05.2018	Ersterstellung
1.1	10.07.2018	Punkt 12.7 neu aufgenimmen
		Anlage 2 - Vertraulichkeit - Pseudonymisierung - Text geändert
		Anlage 2 - Vertraulichkeit - Anonymisierung - hinzugefügt
		Dieses Changelog aufgenommen
2.0	09.10.2019	Zusammenfassung alter Leistungen (1.1) in einem Dokument
		SSL-Lieferant geändert, alt: Comodo neu: Sectigo
		Anschrift SPIEGLHOF media geändert (neuer Firmensitz)
2.1	29.11.2019	Punkt 4. Webentwicklung bei Auftragsgegenstand hinzugefügt