Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Auftraggeber (Verantwortlicher)

Firma:

Straße + Hausnummer:

PLZ + Ort:

Hauptvertragsnummer bzw. Kundennummer:

Auftragnehmer (Auftragsverarbeiter)

Heinlein Consulting GmbH

Schwedter Straße 9a

10119 Berlin

Deutschland

1. Gegenstand und Dauer der Vereinbarung

1. Der Inhalt des Auftrags ergibt sich aus der Leistungsbeschreibung oder dem SLA des Hauptvertrages der vereinbarten Dienstleistung und den Allgemeinen Geschäftsbedingungen, die Bestandteil des Hauptvertrages sind.
2. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.
3. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.

Dauer des Auftrags

1. Die Verarbeitung der Daten beginnt mit dem Abschluss des Hauptvertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses AV-Vertrags oder des Hauptvertrags durch eine Partei.
2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will

oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Durch Kündigung des AV-Vertrags erlischt gleichzeitig der Hauptvertrag und damit die Verarbeitung der Daten.

3. Nach Abschluss der Verarbeitungsleistung wird der Auftragnehmer sämtliche in seinem Besitz sowie an Unterauftragnehmer gelangte Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, entweder dem Auftraggeber aushändigen, oder datenschutzgerecht löschen bzw. vernichten. Der Auftraggeber hat hier das Wahlrecht. Ausgenommen davon sind Dokumentationen, die dem Nachweis des Auftrags und der ordnungsgemäßen Datenverarbeitung dienen, oder denen rechtliche Regelungen oder Pflichten, oder gerichtliche Verfügungen entgegen stehen.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

Die Daten werden auf folgende Arten verarbeitet:

- Erheben, Erfassen, Organisation, Ordnen, Speichern, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschung oder Vernichtung.

Zweck der Verarbeitung ist die Erbringung der Leistungen aus dem Hauptvertrag.

Art der Daten

- Personenstammdaten (z.B. Anrede, Vor- und Nachname, Anschrift)
- Vertragsstammdaten (z.B. Vertragsbeziehung, Produkte/Leistungen)
- Kommunikationsdaten (z.B. Telefonnummer, Mailadressen)
- Abrechnungs- und Zahlungsdaten
- Inhaltsdaten der Datenkommunikation, die über uns abgewickelt wird (z.B. E-Mails, Video- und Audio-Daten, Kalender- und Adressbucheinträge, Daten des Online-Speichers)

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Alle Personen, die Dienste aus dem Hauptvertrag nutzen
- Alle Personen, über die kommuniziert wird
- Kunden und Interessenten
- Mitarbeiter
- Geschäftspartner und Lieferanten
- Interessenten
- Handelsvertreter
- Ansprechpartner

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format durch den Auftraggeber zu bestätigen.
4. Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1. Weisungsberechtigte Personen des Auftraggebers: entsprechen den in den Stammdaten des Kundenaccounts genannten Personen.
2. Weisungsempfänger beim Auftragnehmer sind: alle Administratoren der Firma Heinlein Support GmbH
3. Für Weisung zu nutzende Kommunikationskanäle: Support-E-Mail-Adressen bzw. Helpdesk-Ticketsystem des jeweiligen Geschäftsbereiches (siehe Hauptvertrag). In dringenden Ausnahmen Support-Hotline des jeweiligen Geschäftsbereiches (siehe Hauptvertrag)
4. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre durch beide Vertragspartner aufzubewahren.

5. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
5. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO).
6. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
7. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt.
8. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
9. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO) durchzuführen.
10. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
11. Die Verarbeitung von Daten im Auftrag des Verantwortlichen findet grundsätzlich in den Betriebsstätten des Auftragsverarbeiters statt. Zur Sicherstellung der Serverfunktion und Hilfe bei Notfällen arbeiten die unter **Punkt 4.2** genannten Personen vor allem während der Rufbereitschaft mobil und im HomeOffice und verarbeiten dort Daten. Als Datenverarbeitungsgeräte

kommen ausschließlich Firmen-Rechner zum Einsatz, die entsprechend abgesichert sind. Der Transport der Daten erfolgt ausschließlich über verschlüsselte Verbindungen (VPN-Tunnel).

12. Der Auftragnehmer verpflichtet sich, die Zugriffe im Rahmen dieser Ausnahmen auf das notwendige Maß zu begrenzen und angemessene Sicherheitsmaßnahmen für die technischen Zugriffe zu implementieren. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.
13. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
14. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
15. Handelt es sich beim Auftraggeber um eine Berufsgruppe, die nach § 203 StGB einer besonderen Schweigepflicht unterliegt, so verpflichtet sich der Auftragnehmer auch die für den Auftrag relevanten Geheimschutzregeln (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.) zu beachten. Der Auftragnehmer ist zur Verschwiegenheit über alle Tatsachen verpflichtet, die dem Auftraggeber bekannt geworden sind und zu denen der Auftraggeber ihm den Zugang eröffnet hat. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Auftragnehmer ist ferner verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist. Er ist ebenso verpflichtet, von ihm beschäftigte Personen, die er zur Vertragserfüllung heranzieht, in schriftlicher Form zur Verschwiegenheit zu verpflichten. Der Auftragnehmer ist befugt, Subunternehmer zur Vertragserfüllung heranzuziehen. In diesem Fall ist der Auftragnehmer verpflichtet sicher zu stellen, dass sich der Subunternehmer ebenfalls auf die Geheimhaltung verpflichtet. Auf die strafrechtlichen Folgen der Verletzung dieser Pflichten wurde hingewiesen, insbesondere auf §§ 203 und 204 StGB. Dem Auftragnehmer ist bekannt, dass diese Strafvorschrift auch für ihn und seine Mitarbeiter gilt. Die Vorschriften über den Schutz personenbezogener Daten bleiben hiervon unberührt.
16. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
17. Der Auftragnehmer stellt dem Auftraggeber, oder einem vom Auftragnehmer beauftragten Prüfer, alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Vertrag getroffenen

Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

1. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer generell gestattet, Art. 28 Abs. 2 DSGVO. Der Auftragnehmer muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.
2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
3. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
4. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).
5. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.
6. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
7. Zurzeit sind für den Auftragnehmer die in **Anlage 02** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
8. Der Auftragnehmer informiert den Auftraggeber immer mindestens 14 Tage vorher über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Der Auftraggeber kann mit einer Frist von 14 Tagen gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO), sofern ein sachlicher Grund vorliegt.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO derart berücksichtigt, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer eingedämmt wird. Bei der Festlegung der Maßnahmen werden der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zweck der Verarbeitung berücksichtigt, ebenso wie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Die Schutzziele und Maßnahmen im Einzelnen sind in **Anlage 01** beschrieben.
2. Die beim Auftragnehmer getroffenen Maßnahmen müssen in jedem Fall den Anforderungen des Art. 32 DSGVO entsprechen, sodass Anlage 01 nur einen nicht abschließenden Mindeststandard definiert. Die Maßnahmen werden im Laufe des Auftragsverhältnisses jeweils der technischen und organisatorischen Weiterentwicklung und Erfordernissen angepasst, dürfen aber die in Anlage 01 vereinbarten Standards und die Anforderungen des Art. 32 DSGVO nicht unterschreiten.
3. Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen und die Maßnahmen ggf. dynamisch anzupassen. (Art. 32 Abs. 1 lit. d DSGVO). Ebenso werden die technischen und organisatorischen Maßnahmen der Subunternehmer des Auftragnehmers aus gegebenem Anlass, oder mind. ein mal jährlich überprüft. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Auftraggeber jederzeit auf Verlangen vorzulegen.
4. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

10. Vergütung

1. Die Vergütung wird im Hauptvertrag geregelt. Eine gesonderte Vergütung im Rahmen dieses Vertrages erfolgt nicht.

11. Haftung

1. Haftung und Schadenersatz sind in Art. 82 DSGVO geregelt.

12. Sonstiges

1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
2. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
3. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlagenverzeichnis

Anlage 01: Technische und organisatorische Maßnahmen des Auftragsverarbeiters zur Gewährleistung der Sicherheit der Datenverarbeitung nach Art. 32 DSGVO

Anlage 02: Unterauftragsverhältnisse gemäß 7 der Vereinbarung zur Auftragsverarbeitung

Anlage 03: Zusatzvereinbarung für Berufsgeheimnisträger nach § 43e BRAO

Anlagen

Anlage 01:
Technische und organisatorische Maßnahmen (TOM) des Auftragsverarbeiters zur Gewährleistung der Sicherheit der Datenverarbeitung nach Art. 32 DSGVO

Maßnahmen zur Pseudonymisierung und Verschlüsselung

Technisch

- Verschlüsselung von Datenträgern auf mobilen, und wo umsetzbar auch auf stationären Systemen
- Verschlüsselte Übertragung und Speicherung von Zugangsdaten
- Verschlüsselte Datenübertragung über Netzwerke (E-Mail, PGP, HTTPS)

Organisatorisch

- Regelmäßige Schulung der Mitarbeiter um Umgang mit Verschlüsselungstechniken
- Regelmäßige Kontrolle der Verschlüsselung von Datenträgern und Systemen
- Regelmäßige Kontrolle und ggf. Aktualisierung von Verschlüsselungsverfahren

Maßnahmen zur Sicherstellung der Vertraulichkeit

Technisch

- Alarmanlage in den Geschäftsräumen und im Rechenzentrum mit Anschluss an Notrufzentrale
- Automatisches Zugangskontrollsystem im Rechenzentrum
- Aktenvernichtung durch datenschutzkonforme Aktenvernichter
- Datenträgervernichtung durch mechanische Zerstörung und/oder zertifiziertes Entsorgungsunternehmen
- Chipkarten-/Transponder-Schließsystem in den Büroräumen und im Rechenzentrum
- Schließsystem mit Codesperre in den Bürogebäuden und im Rechenzentrum
- Manuelles Schließsystem in den Bürogebäuden
- Biometrische Zugangssperren im Rechenzentrum
- Videoüberwachung der Zugänge im Rechenzentrum, in den Büroräumen und im Büro-EDV-Raum
- Bewegungsmelder in den Büroräumen
- Sicherheitsschlösser in den Büroräumen

Organisatorisch

- Schlüsselregelung- und Protokollierung in den Büroräumen und im Rechenzentrum
- Protokollierung der Besucher im Rechenzentrum
- Sorgfältige Auswahl von Reinigungspersonal in den Büroräumen
- Tragepflicht von Berechtigungsausweisen im Rechenzentrum
- Passwörter werden ausschließlich von Benutzern erstellt
- Passwörter werden nach Passwort-Richtlinie erstellt
- Jeder Systemzugriff wird protokolliert
- Netzwerk und Server sind durch Firewalls geschützt
- Netzwerke sind separiert
- E-Mails werden nach Möglichkeit verschlüsselt
- Datenträger werden nach Möglichkeit verschlüsselt
- Datenspeicherung auf mobilen Endgeräten erfolgt ausschließlich verschlüsselt
- Fernzugriffe erfolgen ausschließlich über gesicherte Verbindungen (VPN, SSH, TLS)
- Daten für unterschiedliche Zwecke werden - wenn technisch möglich - an getrennten Orten gespeichert.
- Alle Mitarbeiter mit Zugriff auf personenbezogene Daten haben sich gesondert zum Datenschutz und zur Verschwiegenheit verpflichtet
- Zutritt zu den Serverräumen im Rechenzentrum haben nur ausgewählte und fachlich spezialisierte Mitarbeiter
- Mit allen Auftragsverarbeitern wird eine schriftliche Vereinbarung zur Auftragsverarbeitung geschlossen
- Es besteht ein Konzept zur Datenlöschung für alle Systeme
- Es finden regelmäßig Schulungen zum Datenschutz und zur Datensicherheit statt
- Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

Maßnahmen zur Sicherstellung der Integrität

Technisch

- Jede Dateneingabe- und Änderung wird technisch protokolliert.
- Jede Administrationstätigkeit auf DV-Systemen wird technisch protokolliert.
- Zum Validieren von Daten werden Prüfsummen oder ähnliche Methoden eingesetzt.

Organisatorisch

- Es gibt ein Rollen- und Berechtigungskonzept zur Eingabe von Daten.
- Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DSGVO und die Einhaltung von Weisungen sicherzustellen.
- Arbeitsanweisungen zur Gewährleistung der Datensicherheit und der korrekten Ausführung von Aufträgen werden regelmäßig überwacht.
- Datenverarbeitungsprozesse werden regelmäßig durch Tests und/oder Stichprobenkontrollen auf korrekte Funktion überprüft.
- Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

Maßnahmen zur Sicherstellung der Verfügbarkeit und Wiederherstellung

Technisch

- Regelmäßige systematische Datensicherungen
- Regelmäßige Tests der Wiederherstellbarkeit gesicherter Daten (Backups)
- Redundante Auslegung relevanter technischer Systeme
- Unterbrechungsfreie Stromversorgung im Rechenzentrum und Büro-EDV-Raum
- Klimatisierung im Rechenzentrum und Büro-EDV-Raum
- Notstromversorgung der Server im Rechenzentrum
- Anschluss der Server an zwei redundante Stromkreise im Rechenzentrum (wo technisch möglich)
- Anschluss an mehrere redundante Internet-Uplinks im Rechenzentrum
- Automatische Temperaturüberwachung in Serverräumen
- Automatische Überwachung zentraler IT-Systeme
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Redundanter Aufbau der Netzwerk-Infrastruktur im Rechenzentrum
- Sicherung der Netzwerkinfrastruktur durch Firewalls und Anomalieerkennung

Organisatorisch

- Zentrale Beschaffung und/oder Freigabe von Hardwarekomponenten mit langer Verfügbarkeit
- Zentrale Beschaffung und/oder Freigabe von Software mit langer Verfügbarkeit
- Auswahl von Hardwarelieferanten mit langen Service- und/oder Austauschverträgen
- Regelmäßige - wo möglich automatische - Installation von Sicherheitsupdates
- Automatische Überwachung von Ablaufdaten der Server-Betriebssysteme
- IT-Systeme werden durch Fachkräfte betreut, sich dich regelmäßig fortbilden
- Aufbewahrung von Datensicherungen an sicheren, ausgelagerten Orten
- Ein Ausweich-Rechenzentrum für zentrale Anwendungen ist verfügbar
- Einsatz eines doppelten 24/7-Notfalldienstes durch unsere Administratoren
- Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

Maßnahmen zur Sicherstellung der Belastbarkeit

Technisch

- Verfügbarkeit und Auslastung der IT-Systeme wird 24/7 überwacht
- Loadbalancing für zentrale IT-Dienste
- Mehrere Datenleitungen zur Anbindung an das Internet
- Einsatz von Computerclustern mit dynamisch verfügbaren Ressourcen (Rechenkapazität, Speicherplatz)

Organisatorisch

- Regelmäßige Belastungstests der Datenverarbeitungs-Systeme
- Regelmäßige Prüfung der Auslastung der IT-Systeme
- System- und Kapazitätenplanung mit Sicherheitsreserven

- Regelmäßige Prüfung und Überarbeitung der TOM zur Anpassung an aktuellen Stand der Maßnahmen

Anlage 02:
Unterauftragsverhältnisse gemäß Abs. 7 der Vereinbarung zur Auftragsverarbeitung

Die folgenden Unternehmen sind die Betreiber unserer Rechenzentren und in diesem Sinne Subunternehmen. Sie haben jedoch keinen Auftrag zur Datenverarbeitung. Sie stellen ausschließlich die Infrastruktur im Rechenzentrum (Strom, Datenanbindung, Serverschränke, Klimatisierung) zur Verfügung.
Da die rechtliche Stellung im Sinne des Datenschutzes nicht eindeutig geklärt ist, haben wir zur Sicherheit hier ebenfalls AV-Verträge abgeschlossen.

Firma: IPB Internet Provider in Berlin GmbH, Lützowstraße 106, 10785 Berlin

Zwecke: Bereitstellung Infrastruktur im Rechenzentrum (Strom, Netzanbindung, Klimatisierung, Serverschränke

TOM:

- Zutritt nur durch registrierte und zugelassene Personen
- Zutrittskontrollen durch persönliche Anmeldung, Transponder und PIN
- Geschulte Mitarbeiter
- Zertifizierung nach ISO 27001
- AV-Vertrag und Verschwiegenheitsvereinbarung mit Subunternehmer abgeschlossen.

Firma: PlusServer GmbH, Hohenzollernring 72, 50672 Köln

Zwecke: Bereitstellung Infrastruktur im Rechenzentrum (Strom, Netzanbindung, Klimatisierung, Serverschränke)

TOM:

- Zutritt nur durch registrierte und zugelassene Personen
- Zutrittskontrollen durch Transponder, PIN und biometrische Kontrollsysteme
- Geschulte Mitarbeiter
- Zertifizierung nach ISO 27001
- AV-Vertrag und Verschwiegenheitsvereinbarung mit Subunternehmer abgeschlossen.

Anlage 03:
Zusatzvereinbarung für Berufsgeheimnisträger nach § 43e BRAO

Ist der Auftraggeber ein Berufsgeheimisträger, so verpflichtet sich der Auftragnehmer zu ergänzenden Geheimhaltungspflichten. Voraussetzung dafür ist, dass der

Auftraggeber sein Kundenkonto beim Auftragnehmer entsprechend gekennzeichnet hat.

Ergänzend zu den Pflichten aus Ziff. 5 des zwischen den Parteien geschlossenen Auftragsverarbeitungsvertrages vereinbaren die Parteien daher nachfolgende ergänzende Geheimhaltungspflichten, um dem Auftraggeber zu ermöglichen, technische Dienstleistungen i.S.d. § 43e BRAO für Rechtsanwälte erbringen zu können.

Ergänzende Geheimhaltungspflichten

1. Sofern der Auftraggeber als sog. Berufsgeheimnisträger der Schweigepflicht i.S.d. § 203 StGB unterliegt und Leistungen des Auftragnehmers im Zusammenhang mit Tätigkeiten stehen, die der Schweigepflicht des § 203 StGB unterliegen, gilt Folgendes:
2. Dem Auftragnehmer ist bekannt, dass auch für ihn in diesen Fällen nach § 203 Abs. 4 StGB die Schweigepflicht gilt und jede Verletzung der Schweigepflicht nach § 203 StGB strafbar ist. Ferner ist dem Auftragnehmer bekannt, dass die Verwertung von diesen Geheimnissen i.S.d.
   § 203 StGB nach § 204 StGB strafbar ist.
3. Der Auftragnehmer ist verpflichtet, sich nur soweit Kenntnis von fremden Geheimnissen i.S.d.
   § 203 StGB zu verschaffen, wie dies zur Erfüllung der vertraglichen Leistungen gegenüber dem Auftraggeber erforderlich ist.
4. Sofern der Auftragnehmer Unterauftragnehmer einsetzt, ist dieser verpflichtet, Unterauftragnehmer in gleicher Weise auf die Verschwiegenheitspflichten des § 203 StGB zu verpflichten, soweit diese im Rahmen ihrer Dienstleistung Zugriff auf Informationen erhalten könnten, die der Schweigepflicht nach § 203 StGB unterliegen.
5. Die Regelungen des Absatzes 1 gelten entsprechend, wenn der Auftraggeber Leistungen für Rechtsanwälte oder andere Berufsgeheimnisträger erbringt und insoweit Leistungen des Auftragnehmers in Anspruch nimmt.

Unterschriften der Vertragspartner:

Auftragnehmer:

Heinlein Consulting GmbH

vertreten durch Geschäftsführer Peer Heinlein

Auftraggeber:

Datum, Name, Unterschrift