Auftragsverarbeitungsvertrag nach Artikel 28 Abs.3 DS-GVO

Auftraggeber (Verantwortlicher):

Auftraggeber ist der Vertragspartner aus dem Hauptvertrag der gebuchten Dienstleistung.

Auftragnehmer (Auftragsverarbeiter):

Heinlein Support GmbH

Schwedter Straße 8/9B

10119 Berlin

Deutschland

Zm Unternehmen des Auftragnehmers gehören die Marken

- mailbox.org https://mailbox.org
- JPBerlin https://www.jpberlin.de
- Heinlein Hosting https://www.heinlein-hosting.de
- Heinlein Consulting https://www.heinlein-consulting.de
- Heinlein Akademie https://www.heinlein-akademie.de
- ox.io https://ox.io

Für diese Marken ist die Heinlein Support GmbH der Auftragsverarbeiter im Sinne der DSGVO.

1. Gegenstand und Dauer der Vereinbarung

Der Gegenstand des Auftrags ergibt sich aus der Leistungsbeschreibung oder dem SLA des Hauptvertrages der vereinbarten Dienstleistung.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Vorausset- zungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

Die Dauer des Auftrages richtet sich nach der Dauer des Hauptvertrages.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmun- gen 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 DS-GVO abge- leiteten Pflichten stellt einen schweren Verstoß dar.

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 DS-GVO):

Die Art der Verarbeitung richtet sich nach den im Hauptvertrag gebuchten Leistungen. Je nach Geschäftsbereich sind das folgende Arten der Verarbeitung:

- Hosting eines od. mehrerer Root-Server (Heinlein Hosting)
- Hosting eines JPBerlin-Accounts (Shared-Webservice, Postfächer, Mailinglisten)
- Hosting eines mailbox.org Accounts (Postfächer, Adressbuch, Kalender, Aufgaben, Dateien/Drive, Chat)
- Server-Management (Heinlein-Hosting)
- Backup (Heinlein Hosting)

Kategorien der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

Die Kategorien der zu verarbeitenden Daten richtet sich nach den im Hauptvertrag gebuchten Leistungen. Je nach Leistung werden eine oder mehrere der folgende Kategorien verarbeitet:

- Vertragsstammdaten
- Personenstammdaten
- Protokolldateien
- Kommunikationsdaten
- Abrechnungsdaten

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter des Auftraggebers
- Geschäftspartner und Lieferanten des Auftraggebers

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO 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.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

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 zu bestätigen.

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.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

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

Weisungsberechtigte Personen des Auftraggebers:

- entsprechen den in den Stammdaten des Kundenaccounts genannten Personen.

Weisungsempfänger beim Auftragnehmer sind:

- alle Administratoren der Firma Heinlein Support GmbH

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)

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 aufzubewahren.

5. Pflichten des Auftragnehmers

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 DS-GVO).

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.

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.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen 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 DS-GVO).

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 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

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.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO) durchzuführen.

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten im Auftrag des Verantwortlichen findet grundsätzlich in den Betriebsstätten des Auftragsverarbeiters statt. Zur Sicherstellung der Serverfunktion ind Hilfe bei Notfällen arbeiten die unter 4 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 erfolg ausschließlich über verschlüsselte Verbindungen (VPN-Tunnel).

Der Auftragsverarbeiter verpflichtet sich jedoch, 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 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

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.

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 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Datenschutzbeauftragter

Beim Auftragnehmer ist ein betrieblicher Datenschutzbeauftragter bestellt. Sie erreich ihn unter

Tel.: +49 30 40 50 51-41,

E-Mail: privacy@heinlein-support.de

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

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

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag 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 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO 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 DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer generell gestattet, Art. 28 Abs. 2 DS-GVO. 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 DS-GVO sorgfältig auswählt.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

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, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

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.

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.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

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

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 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer eingedämmt wird.

Das im Anhang 01 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maß- nahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).

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 DS-GVO

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

Die Vergütung wird im Hauptvertrag geregelt.

11. Haftung

Haftung und Schadenersatz sind in Art. 82 DS-GVO geregelt.

12. Sonstiges

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.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

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.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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 Auftragsdatenverarbeitung

Anlagen

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

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

Technisch

- Regelmäßige systematische Datensicherungen
- Unterbrechnungsfreie 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 7 der Vereinbarung zur Auftragsdatenverarbeitung

Firma	Zweck	Daten-kategorien	Betroffene Personengruppen	Rechtsgrund-lage	TOM
CPS Datensysteme GmbH Gilgenborn 44 56179 Vallendar Deutschland	Registrierung von Domains im Kundenauftrag	Adressdaten des Domainin-habers	Kunden von JPBerlin und Heinlein Hosting	Vertrag (Auftrag des Kunden)	Gesicherte Datenübertragung (HTTPS) Geschulte Mitarbeiter AV-Vertrag mit Auftragsverarbeiter
PSW GROUP GmbH & Co.KG Flemingstraße 20-22 36041 Fulda Deutschland	Registrierung von SSL-Zertifikaten im Kundenauftrag	Adressdaten des Zertifikatsin-habers	Kunden von JPBerlin und Heinlein Hosting	Vertrag (Auftrag des Kunden)	Gesicherte Datenübertragung (HTTPS) Geschulte Mitarbeiter AV-Vertrag mit Auftragsverarbeiter

Unterschriften der Vertragspartner

Auftragnehmer:

Heinlein Support GmbH

vertreten durch Geschäftsführer Peer Heinlein

Auftraggeber:

Datum und Unterschrift Auftraggeber