

Vereinbarung zur Auftragsverarbeitung gem. Art. 28 EU-Datenschutzgrundverordnung (DS-GVO)

zwischen

- nachfolgend „**Auftraggeber**“ genannt -

und

Taskworld Deutschland GmbH,
c/o Mindspace, Friedrichstraße 68, 10117 Berlin Deutschland

- nachfolgend „**Auftragnehmer**“ genannt -

- Auftraggeber und Auftragnehmer nachfolgend jeweils eine
„**Partei**“ und gemeinsam die „**Parteien**“ -

INHALTSVERZEICHNIS

| Klausel | Seite |
|---|-------|
| 1. Vertragsgegenstand und Auftragsinhalt | 3 |
| 2. Technische und organisatorische Maßnahmen | 3 |
| 3. Berichtigung, Einschränkung und Löschung von Daten | 4 |
| 4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers | 4 |
| 5. Unterauftragsverhältnisse | 5 |
| 6. Kontrollrechte des Auftraggebers | 6 |
| 7. Weisungsbefugnis des Auftraggebers | 7 |
| 8. Löschung und Rückgabe von personenbezogenen Daten | 7 |
| 9. Auftragsdauer, Kündigung | 8 |
| 10. Anwendbares Recht, Erfüllungsort, Gerichtsstand | 8 |
| 11. Sonstiges | 9 |
| Anlage | 10 |
| Anlage 1 – Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen | 11 |
| Anlage 2 – Technische und organisatorische Maßnahmen | 12 |

1. Vertragsgegenstand und Auftragsinhalt

1.1 Der Gegenstand des Vertrags ergibt sich aus der zwischen den Parteien abgeschlossenen Vereinbarung über die Zurverfügungstellung einer Services des Auftragnehmers an den Auftraggeber , auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“). Dieser Vertrag zur Auftragsverarbeitung (der „Vertrag“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien. Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit der Auftragsverarbeitung in Zusammenhang stehen und bei denen der Auftragnehmer oder dessen Mitarbeiter mit personenbezogenen Daten, die dem Auftragnehmer vom Auftraggeber übermittelt werden, in Berührung kommen können.

1.2 Die Art der verarbeiteten Daten, die Kategorien betroffener Personen und die Art und der Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Detail in der Anlage 1 zu diesem Vertrag festgelegt.

1.3 Soweit in diesem Vertrag nicht ausdrücklich anders bestimmt, findet die Erbringung der vertraglich vereinbarten Datenverarbeitung ausschließlich in Deutschland, einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die einzelnen Maßnahmen dokumentiert der Auftragnehmer in einem Maßnahmenkonzept in Anlage 2.

2.1 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

2.2 Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

3. Berichtigung, Einschränkung und Löschung von Daten

3.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.2 Der Auftragnehmer wird den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen darin unterstützen, die Rechte Betroffener auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sicherzustellen. Für Unterstützungsleistungen, die nach der Leistungsvereinbarung nicht geschuldet sind, kann der Auftragnehmer eine Vergütung beanspruchen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

4.1 Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht worden sind. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisungen des Auftraggebers, einschließlich der in diesem Vertrag und der Leistungsvereinbarung eingeräumten Befugnisse, verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

4.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32-36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören unter anderem:

- 4.2.1 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- 4.2.2 die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber den Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
- 4.2.3 die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgeabschätzung.
- 4.2.4 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultation mit der Aufsichtsbehörde.

4.3 Für Unterstützungsleistungen, die nicht in der Leistungsvereinbarung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

5. Unterauftragsverhältnisse

5.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer zum Beispiel als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

5.2 Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern unter der Bedingung einer vertraglichen Vereinbarung zwischen dem Auftragnehmer und dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 4 DS-GVO zu. Die Zustimmung umfasst, vorbehaltlich der vorgenannten Bedingung, ausdrücklich den Einsatz der nachfolgend benannten Unterauftragnehmer.

5.3 Der Auftragnehmer nimmt Infrastruktur- und Plattformdienstleistungen der von der Amazon Web Services, Inc. betriebenen Amazon Web Services Plattform für die Bereitstellung der Softwarelösung gem. Leistungsvereinbarung in Anspruch. Die Verarbeitung erfolgt auf einem Server der Amazon, Inc. in Frankfurt / Main (Deutschland). Über die Nutzung des Dienstes Amazon Web Services sowie die Auftragsverarbeitung bestehen Verträge zwischen Taskworld und Amazon Web Services, Inc., die Amazon Web Services, Inc. zum Schutz personenbezogener Daten verpflichten. Detaillierte Informationen der Amazon Web Services, Inc. über die Einhaltung der datenschutzrechtlichen Anforderungen durch Amazon Web Services, Inc. finden sich unter <https://aws.amazon.com/de/compliance/eu-data-protection/>.

5.4 Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter. Der Auftraggeber kann dieser Änderung gegenüber dem Auftragnehmer innerhalb von 14 Tagen ab Eingang der Information beim Auftraggeber widersprechen. Ein Widerspruch darf nicht ohne ein die Interessen des Auftragnehmers überwiegendes Interesse des Auftraggebers erfolgen.

5.5 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6. Kontrollrechte des Auftraggebers

6.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

6.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

6.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- 6.3.1 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO,
- 6.3.2 die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO,
- 6.3.3 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zum Beispiel Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditorium, Qualitätsaudit),
- 6.3.4 eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (zum Beispiel nach BSI-Grundschutz).

6.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

7. Weisungsbefugnis des Auftraggebers

7.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).

7.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung auszusetzen bis sie durch den Auftraggeber bestätigt oder geändert wird.

8. Löschung und Rückgabe von personenbezogenen Daten

8.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie die Aufbewahrung von Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich ist.

8.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Die Pflichten des Auftragnehmers nach dieser Ziffer 8.2 gelten nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten der EU eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8.3 Dokumentationen, die dem Nachweis der auftragsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9. Auftragsdauer, Kündigung

9.1 Die Dauer dieses Auftrags entspricht der Dauer der Leistungsvereinbarung und schließt darüber hinaus den Zeitraum nach Ende des Leistungsvereinbarung bis zur vollständigen Rückgabe oder Löschung der vom Auftraggeber im Zusammenhang mit der Durchführung des Hauptvertrages dem Auftragnehmer überlassenen Daten ein.

9.2 Unberührt bleibt das Recht jeder Vertragspartei, diesen Auftrag aus wichtigem Grund fristlos zu kündigen.

10. Anwendbares Recht, Erfüllungsort, Gerichtsstand

10.1 Auf vorliegenden Vertrag findet deutsches Recht Anwendung.

10.2 Erfüllungsort ist Berlin.

10.3 Für Streitigkeiten aus diesem Vertrag ist ausschließlicher Gerichtsstand Berlin.

11. Sonstiges

11.1 Änderungen, Ergänzungen und Zusätze dieses Vertrags haben nur Gültigkeit, wenn sie zwischen den Vertragsparteien schriftlich vereinbart werden. Dies gilt auch für die Abänderung dieser Vertragsbestimmung.

11.2 Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Die unwirksame Bestimmung gilt als durch eine wirksame Regelung ersetzt, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Entsprechendes gilt im Fall einer Vertragslücke.

Anlagen:

Anlage 1: Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

Anlage 2: Technische und organisatorische Maßnahmen

Berlin, 25. Mai 2018

[Ort], [Datum]



Taskworld Deutschland GmbH

Patrick Wings

Geschäftsführer

Anlage 1 – Art und Zweck der Verarbeitung, Art der Daten, Kreis der Betroffenen

| | |
|---|---|
| Betroffene Personen und Personengruppe | Betroffene Personen und Personengruppe Insbesondere: Nutzer/Anwender der bereitgestellten Software-Lösung Vertragspartner des Auftraggebers Mitarbeiter des Auftraggebers Interessenten. |
| Art der Daten oder Datenkategorien | Insbesondere: Personenstammdaten Kommunikationsdaten (zB Telefon, E-Mail) Vertragsstammdaten Vertragsabrechnungs- und Zahlungsdaten Kundenhistorie Planungs- und Steuerungsdaten. |
| Empfänger | Auftragnehmer Unterauftragnehmer |
| Art und Zweck der Verarbeitung | Zurverfügungstellung der Software mit Speicherplatz über das Internet; Erbringung von IT-Dienstleistungen, insbesondere Supportleistungen |

Anlage 2 – Technische und organisatorische Maßnahmen

Vorbemerkung: Die Taskworld Deutschland GmbH (nachfolgend „Taskworld“) verarbeitet im Rahmen dieses Vertrags personenbezogene Daten ausschließlich zur Erfüllung von Service- und Supportverpflichtungen aus der Leistungsvereinbarung. Sämtliche Daten liegen auf der Amazon Web Services Plattform (s. Ziffer 5.2 des Vertrags; nachfolgend „AWS-Plattform“ genannt). Taskworld greift auf die Daten über einen hierzu bereitgestellten Laptop oder Desktop durch den mit der Leistungserbringung betrauten Arbeitnehmer zu. Über die Nutzung des Dienstes Amazon Web Services besteht ein Vertrag zwischen Taskworld und Amazon Web Services, Inc. Detaillierte Informationen der Amazon, Inc. über die Einhaltung der datenschutzrechtlichen Anforderungen durch Amazon, Inc. finden sich unter <https://aws.amazon.com/de/compliance/eu-data-protection/>. Nachfolgend werden die technischen und organisatorischen Maßnahmen der Taskworld beschrieben.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zugangskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Der einzige Rechner mit Zugang zu Daten des Auftraggebers wird in verschlossenen Räumen aufbewahrt.
- Der Zutritt zu diesen Räumen ist nur dem für Support zuständigen Arbeitnehmer gewährt, solange der Rechner eingeschaltet ist.
- Der Rechner ist zusätzlich durch ein Kensington Schloss gesichert.
- Über einen Schlüssel zum Kensington Schloss verfügt allein der für den Support zuständige Arbeitnehmer.

1.2 Datenträgerkontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern:

- Zur Datensicherung verwendete externe Datenträger werden separat aufbewahrt und durch ein zusätzliches Schloss gesichert.
- Über den Schlüssel zum Datenträger verfügen nur Arbeitnehmer.

1.3 Zugriffs-, Speicher- und Benutzerkontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

- Es wird nur ein Rechner mit Zugang zu Daten des Auftraggebers eingerichtet, welcher ausschließlich zum Zweck der Erbringung von Support-Leistungen für die Softwarelösung des Auftragnehmers verwendet wird.
- Dieser Rechner ist mit einem qualifizierten Passwort, welches aus mind. 8 Zeichen, darunter jeweils mind. ein Sonderzeichen und eine Ziffer, gesichert.
- Das Passwort wird im 2-monatigen Rhythmus geändert.
- Bei Abwesenheit des Arbeitnehmers vom Rechner wird sofort die Passwortsperre aktiviert.
- Externe Sicherungskopien auf Datenträgern werden gleichermaßen passwortgesichert. Es darf nicht dasselbe Passwort für den Rechner und den Datenträger verwendet werden.
- Zugriff auf Datenverarbeitungssysteme ist allein dem für Support zuständigen Arbeitnehmer gestattet.
- Dies wird durch Benutzerprofil mit Kennwort- und Passwortsicherung gewährleistet.
- Weitere Berechtigungen zum Zugriff auf Datenverarbeitungssysteme sind nicht vorhanden.

1.4 Trennbarkeit

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Auf die Daten des Auftraggebers wird ausschließlich im Rahmen des Auftrags und zum Zweck der Support-Leistung zugegriffen.
- Der Support leistende Arbeitnehmer des Auftragnehmers verarbeitet die Daten des Auftraggebers getrennt von anderen Daten. Dies wird durch die Einrichtung von Kundenkonten gewährleistet.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Transportkontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Eine Übermittlung/Übertragung von Daten erfolgt ausschließlich verschlüsselt über deutsche Server.
- Eine Übermittlung/Übertragung auf externe Datenträger erfolgt ausschließlich über gesicherte lokale Verbindungen.
- Jede Übermittlung/Übertragung von Daten wird protokolliert.
- Eine Übermittlung/Übertragung erfolgt nur zum Zweck der Sicherung oder zur auftragsgemäßen Datenverarbeitung.

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Mit der Verarbeitung von personenbezogenen Daten des Auftraggebers ist im Rahmen des Supports nur ein Arbeitnehmer des Auftragnehmers betraut.
- Der Arbeitnehmer protokolliert jede Dateneingabe, -änderung oder -entfernung.
- Die Protokolle werden für jeden Support-Vorgang zusammengefasst und in geeigneter Weise zur nachträglichen Überprüfung aufgearbeitet.
- Die aufgearbeiteten Protokolle werden auf Wunsch dem Auftraggeber zur Verfügung gestellt.

2.3 Datenintegrität

Keine Beschädigung von Daten durch Fehlfunktionen des Systems

- Die Integrität der Daten wird durch externe Sicherheitskopien auf Datenträgern gewährleistet.
- Datenverarbeitungssysteme werden im Rahmen der technischen Möglichkeiten so eingerichtet, dass eine Beschädigung oder der Verlust von Daten ausgeschlossen wird.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Der für die Support-Leistungen verwendete Rechner ist mit einem Virenschutz und einer Firewall ausgestattet, die laufend aktualisiert werden.
- Zur Sicherung der Daten wird in regelmäßigen Abständen ein Back-Up auf einem externen Datenträger erstellt.
- Die unterbrechungsfreie Stromversorgung des Rechners und die Verfügbarkeit der Daten werden durch Verwendung von moderner Hardware, die regelmäßig gewartet wird, sichergestellt.

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Nach einer Störung der Datenverarbeitungssysteme werden alle Systemkomponenten unverzüglich auf Fehler überprüft und festgestellt, ob es zu einer Beschädigung von Daten gekommen ist.
- Sofern es zu einer Beschädigung der Daten oder zu einem Datenverlust kam, werden die Daten von einem externen Datenträger wiederhergestellt.
- Ein Bericht über das Ausmaß und die Behebung der Störung wird zur zukünftigen Referenz erstellt.

3.3 Zuverlässigkeit

Verfügbarkeit aller Funktionen des Systems und Fehlermeldung:

- Alle Datenverarbeitungssysteme werden regelmäßig aktualisiert, auf Fehler geprüft und gewartet.
- Es wird regelmäßig geprüft, ob die verwendeten Systeme dem aktuellen technischen Standard entsprechen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management:

- Alle Arbeitnehmer des Auftragnehmers werden über datenschutzrechtliche Themen informiert und zur Einhaltung von datenschutzrechtlichen Vorschriften verpflichtet.
- Die Geschäftsführung des Auftragnehmers prüft in regelmäßigen Abständen, ob die internen Vorgänge datenschutzrechtlichen Vorgaben genügen und ergreift entsprechende Maßnahmen, um dies zu gewährleisten.
- Die Geschäftsführung wird laufend zu datenschutzrechtlichen Fragen anwaltlich beraten.
- Der Zugriff auf die Daten des Auftraggebers durch Arbeitnehmer des Auftragnehmers erfolgt ausschließlich innerhalb Deutschlands und über deutsche Server.

4.2 Incident-Response-Management:

- Im Falle eines Sicherheitsvorfalls, der sich auf die Datenverarbeitungssysteme auswirken könnte, wird die Geschäftsführung des Auftragnehmers von den Arbeitnehmern unverzüglich informiert.
- Eine Datensicherung erfolgt bei Verdacht eines Sicherheitsvorfalls auf einen separaten Datenträger nach jeder Dateneingabe oder -änderung.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Der Auftragnehmer achtet bei der Auswahl der verwendeten Hard- und Software auf ihre Vereinbarkeit mit dem Gebot der Datenminimierung.
- Bei der Installation von Software wird auf Komponenten, die zur Verwendung der Software nicht notwendig sind und zu einer Beeinträchtigung der Daten des Auftraggebers führen können, verzichtet.

4.4 Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

- Der Arbeitnehmer des Auftragnehmers ist vertraglich dazu verpflichtet, dessen Daten entsprechend der Weisungen des Auftraggebers zu verarbeiten.
- Die Befugnisse des Auftragnehmers sind vertraglich deutlich und abschließend geregelt.
- Aufträge und Supportanfragen werden in Textform dokumentiert, um die Auftragslage auch nachträglich nachvollziehen zu können.
- Der für den Support zuständige Arbeitnehmer pflegt einen direkten Kontakt zum Auftraggeber.