

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Zwischen

im Folgenden „Auftraggeber“

und

Fisel GmbH

Gellertstraße 83

74074 Heilbronn

im Folgenden „Auftragnehmer“

§1 Gegenstand und Dauer der Verarbeitung

Der Auftrag umfasst alle Tätigkeiten, die mit dem/den Hauptvertrag/Hauptverträgen in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Als solche Tätigkeiten kommen insbesondere ein Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtzeiten enthaltenden Dump/ Backup-Datei – vor allem im Zusammenhang mit Supportanfragen – in Betracht, soweit auf dem IT-System oder in den Echtzeiten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für die Verarbeitung im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrags.

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 Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Vertrag wird auf unbestimmte Zeit geschlossen und ist mit einer Frist von 31 Tagen kündbar.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftraggeber Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Daten

Art der Verarbeitung (gem. Art. 4 Nr. 2 DS-GVO)

Personenbezogene Daten werden ausschließlich nach Weisung durch einen Weisungsbefugten (§4) verarbeitet.

Hierbei umfasst die Verarbeitung die Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Veränderung, Abfrage, Verwendung, Abgleich und das Löschen, sowie die Vernichtung der personenbezogenen Daten.

Eine Offenlegung durch Übermittlung erfolgt nur im Unterauftragsverhältnis mit einem Subunternehmer und nur nach Rücksprache mit dem Auftraggeber.

Art und Kategorien der Personenbezogenen Daten (gem. Art. 4 Nr. 1, 13, 14, 15 DS-GVO)

Verarbeitet werden Informationen, die einer natürlichen Person eindeutig zugeordnet sind oder einer natürlichen Person eindeutig zugeordnet werden können.

Im Rahmen dieses Vertrages werden nur Daten verarbeitet, die nicht unter die Kategorie besonderer Personenbezogener Daten (gem. Art. 9 Abs. 1 DS-GVO) fallen.

§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 nach Art. 28 Abs. 3 lit. (h) berechtigt die Einhaltung der in diesem Vertrag festgelegten Regelungen und Richtlinien sowie im Besonderen die der festgelegten Rechte und Pflichten des Auftragsverarbeiters, über eine Anforderung der benötigten Informationen oder durch Inspektionen zu überprüfen.

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 sind:

Vorname	Name	Organisationseinheit	Telefonnummer

Weisungsempfangende Personen des Auftragnehmers sind:

Vorname	Name	Telefonnummer
Steffen	Fisel	+49 (0) 7131 120 80 0
Léon	Fisel	+49 (0) 7131 120 80 0
Mike	Grab	+49 (0) 7131 120 80 0

Für Weisungen zu nutzende Kommunikationskanäle:

a) Postalisch
Fisel GmbH
Gellertstraße 83
74074 Heilbronn
Deutschland

b) Telefonisch
+49 (0) 7131 120 80 0

c) E-Mail
info@fisel.de

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.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber regelmäßige, interne Überprüfungen durchzuführen. Das Ergebnis dieser Kontrollen ist zu dokumentieren.

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 berechnete 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 in diesem Vertrag festgelegten Regelungen und Richtlinien sowie im Besonderen die der festgelegten Rechte und Pflichten des Auftragsverarbeiters, im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Hierbei sichert der Auftragnehmer seine Zusammenarbeit mit der kontrollierenden Stelle zu.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen.

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 zudem für den Auftrag relevante Geheimhaltungsregeln, die dem Auftraggeber obliegen zu beachten. Folgendes ist hierbei zusätzlich zu beachten:

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 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

§6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzung 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. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. 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 Unterauftragsverhältnis 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 nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen 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. Dem Auftraggeber muss die Möglichkeit gegeben werden, im Bedarfsfall durch angemessene Überprüfungen und Inspektionen die Einhaltung der Vertraglichen Verpflichtungen 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 hat die Einhaltung der Pflichten der Subunternehmer regelmäßig zu überprüfen und die Ergebnisse dieser zu dokumentieren.

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 3 mit Namen, Anschrift, Kontaktmöglichkeit, Ansprechpartner 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 Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Das im Anhang 1 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.

Das im Anhang 3 beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber alle 24 Monate, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis der Überprüfung ist dem Auftraggeber auf Anfrage mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

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

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§9 Verpflichtung des Auftragnehmers nach Beendigung des Auftrags (gem. 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, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

§10 Haftung

Es wird auf Artikel 82 DS-GVO verwiesen.

§11 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.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort: _____

Ort: Heilbronn


Datum: ____ . ____ . 20 ____

Datum: 01.10. 2018

X

Auftraggeber

X



Auftragnehmer

Anhang 1 – Umfang, Art und Zweck der Datenverarbeitung

Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

Produkt	Betroffene Datenkategorien *	Subunternehmer
Sage 50, Sage 50c	1,2,3,4,5,6	-
Sage GS	1,2,3,4,5,6	-
PCK	1,2,3,4,5,6	-
Sage 50 Adressen	1,3	-
GS Adressen	1,3	-
Betriebsprüferarchiv		Sage, Frankfurt
cobra CRM Plus/Pro, cobra Adressen	1,2,3,8	cobra, Konstanz
Sage Webshop	1,2,4,5	-
Klick-Tipp	1,2,3,8	Klick-Tipp Ltd., London, GB

*Datenkategorien und Personen

1. Kontaktdaten und -historie bzgl. natürlicher Personen d.h. Kunden, Lieferanten, Ansprechpartner von Firmen, Interessenten und Vertretern
2. Daten zur Geschäftshistorie von Kunden, Lieferanten und Vertretern
3. Daten von Mitarbeitern bzw. Anwendern des Systems
4. Daten zu finanziellen Transaktionen von Kunden, Lieferanten und Vertretern
5. Daten zu Bankverbindungen und Zahlungsarten von Kunden, Lieferanten und Vertretern
6. Daten zur Vermögens -und Ertragssituation von Kunden und Lieferanten
7. Daten zu Arbeitszeiten und Abläufen von Mitarbeiter
8. Sonstige (unstrukturierte) personenbezogene Daten von Kunden, Lieferanten, Ansprechpartnern von Firmen, Interessenten, Vertretern, Mitarbeitern und Anwendern des Systems

Soweit eines der o.g. Produkte nicht den Funktionsumfang aufweist, entfallen die Datenkategorien für einige der genannten Personen. Gleichzeitig ist es aber auch in einigen Produkten möglich, individuell die Datenkategorien zu erweitern oder anders als vorgesehen zu nutzen. Dies obliegt gemäß § 4 (2) der Vereinbarung zur Auftragsverarbeitung dem Anwender der Produkte.

Kreis der Betroffenen

Betroffene der Datenverarbeitung sind all diejenigen, deren Daten von Auftraggeber im Rahmen des/der Hauptvertrag/Hauptvertrages an den Auftragnehmer übertragen werden.

Anhang 2 – Technisch organisatorischer Maßnahmen

Um die von ihm verarbeiteten personenbezogenen Daten zu schützen, hat der Auftragnehmer angemessene technische und organisatorische Sicherheitsmaßnahmen, einschließlich der folgenden Maßnahmen umgesetzt:

Pseudonymisierung und Verschlüsselung personenbezogener Daten

- https Verschlüsselung in der Webkommunikation
- Verschlüsselung / Nutzung von VPN-Tunneln bei der Übertragung

Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

- Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern
- Berechtigte können nur auf für sie berechnete Daten zugreifen
- Personenbezogene, gespeicherte Daten können nur im Rahmen des Berechnungskonzeptes gelesen, kopiert, verändert oder entfernt werden.
- Verwendung fortlaufend aktualisierter Virenschutzsoftware
- Schutz des E-Mail-Verkehrs vor Viren und Spam
- Firewall
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Hohe Passwortsicherheit, regelmäßiger Wechsel
- Kein Zutritt für Unbefugte in die Geschäftsräume
- Während der Geschäftszeiten wird der Zutritt zu den Geschäftsräumen durch die Mitarbeiter kontrolliert
- Besucher der Geschäftsräume werden begleitet
- Sichere Löschung von Datenträgern
- Mitarbeiter müssen beim Verlassen des Arbeitsplatzes den Arbeitsplatz sperren
- Sicherstellung einer hohen Widerstandsfähigkeit der DV-Systeme bei starkem Zugriff bzw. starker Belastung, etwa durch Angriffe von außen
- Verwendung ausgetesteter Software
- Trennung der Produktiv- von den Test- und Entwicklungsumgebungen
- Alert-Meldungen bei hohen Belastungen
- Virtualisierungen
- Festlegung der berechtigten Personen in Listen für die sensiblen Bereiche der Server Systeme
- Regelungen zur Beschaffung von Hardware und Software
- Zentrales Rechtemanagement für Arbeitsplatz PC
- Regelung und Kontrolle von externer Wartung und Fernwartung
- Brandschutzvorrichtungen

Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

- Personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch regelmäßiges Backup
- Datensicherungs- und Recoverykonzept
- Sicherheitskopien
- Unterbrechungsfreie Stromversorgung
- Überwachungs- und Meldesysteme

Anhang 3 – Verfahren zur Überprüfung der Technisch organisatorischen Maßnahmen

Der Auftragnehmer ist nach Artikel 32 Abs. 1 lit. d verpflichtet die technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen, und die Wirksamkeit dieser zu evaluieren. Dies wird wie folgt umgesetzt:

- Überprüfung, ob technische und organisatorische Maßnahmen dem aktuellen Stand der Technik entsprechen
- Überprüfung, ob verwendete Software auf dem aktuellen Release Stand sind

- Überprüfung, ob alle aktuellen Patches eingespielt sind
- Überprüfung, ob Viren Schutz und Firewall regelmäßig aktualisiert werden
- Überprüfen, ob die verwendeten Verschlüsselungstechnologien auf dem aktuellen Stand der Technik sind
- Überprüfung, ob verwendete Authentifizierungsverfahren die Systeme vor unbefugtem Zugriff schützen
- Überprüfung, ob die realisierten Protokollierungen ausreichend sind
- Überprüfung, ob die mit der Datenverarbeitung betrauten Personen regelmäßig sensibilisiert und fortgebildet werden
- Überprüfung, ob die erstellten Backups wieder in das System eingespielt werden können
- Überprüfung, ob die organisatorischen Maßnahmen zum Schutz der Büroräume ausreichend sind

Anhang 4 – Liste der Subunternehmer

Gemäß § 7 stimmt der Auftraggeber mit Unterzeichnung des Vertrages zu, dass der Auftragnehmer folgende weitere Auftragsverarbeiter im Rahmen der Datenverarbeitungstätigkeiten einsetzt:

Subunternehmer	Sage GmbH
Adresse	Franklinstraße 61 - 63 60486 Frankfurt/Main
Kontaktmöglichkeit	069/50007-0 info@sage.de Deutschland
Ansprechpartner	Geschäftsführer: Heino Erdmann
Auftragsinhalt	3rd Level Support für die durch den Auftragnehmer vertrieben Produkte der Sage GmbH. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdateien enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdateien personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Subunternehmer	Fisel Solution UG
Adresse	Gellertstraße 83 74074 Heilbronn Deutschland
Kontaktmöglichkeit	07131/12080-60 info@fisel-solution.de
Ansprechpartner	Geschäftsführer: Steffen Fisel
Auftragsinhalt	IT- und Programmiertechnische Dienstleistungen, die mit den Tätigkeiten des/der Hauptvertrages/Hauptverträge in Zusammenhang stehen. Dies beinhaltet Remotezugriff auf das IT-System des Auftragnehmers und des Auftraggebers, der Umgang mit einem Echtdateien enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdateien personenbezogene Daten enthalten sind.

Subunternehmer	cobra – computer´s brainware GmbH
Adresse	Gellertstraße 83 78467 Konstanz Deutschland
Kontaktmöglichkeit	07531/8101-0 info@cobra.de
Ansprechpartner	Geschäftsführer: Jürgen Litz
Auftragsinhalt	3rd Level Support für die durch den Auftragnehmer vertrieben Produkte der cobra – computer´s brainware GmbH. Dies beinhaltet den Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind. Weiterhin fallen hierunter Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Subunternehmer	KLICK-TIPP LIMITED
Adresse	15 Cambridge Court 210 Shepherd´s Bush Road London W6 7NJ Vereinigtes Königreich
Ansprechpartner	Gesetzlicher Vertreter: Michael Toohig, Josef Wolosz
Auftragsinhalt	3rd Level Support für die durch den Auftragnehmer vertrieben Produkte der KLICK-TIPP LIMITED und Hosting von Software, ASP, SaaS oder Cloud basierende Angebote der Softwareüberlassung.

Subunternehmer	maxIcon Melanie Fisel
Adresse	Theodor-Heuss-Straße 51 74223 Flein Deutschland
Kontaktmöglichkeit	07131/12080-90 info@maxicon.de
Ansprechpartner	Melanie Fisel
Auftragsinhalt	Organisationsberatung und Vertriebsdienstleistungen, die mit der Ausführung der vertraglichen und vorvertraglichen Maßnahmen in Zusammenhang stehen. Dies beinhaltet Remotezugriff auf das IT-System des Auftraggebers, der Umgang mit einem Echtdaten, soweit auf dem IT-System oder in den Echtdaten personenbezogene Daten enthalten sind.

Subunternehmer	Fisel Systemtechnik
Adresse	Gellertstraße 83 74074 Heilbronn Deutschland
Kontaktmöglichkeit	07131/205 9 747 info@fisel.de

Ansprechpartner	Geschäftsführer: Steffen Fisel
Auftragsinhalt	IT- und Programmiertechnische Dienstleistungen, die mit den Tätigkeiten des/der Hauptvertrages/Hauptverträge in Zusammenhang stehen. Dies beinhaltet Remotezugriff auf das IT-System des Auftragnehmers und des Auftraggebers, der Umgang mit einem Echtdatei enthaltenden Dump/Backup, soweit auf dem IT-System oder in den Echtdatei personenbezogene Daten enthalten sind.