Vereinbarung gemäß §11 Bundesdatenschutzgesetz (BDSG) zur Auftragsverarbeitung nach DSGVO

zwischen

_____

_____

_____
- nachstehend Auftraggeber genannt -

und der

ASAsoft GmbH
Schönfliesser Str. 78
16548 Glienicke Nordbahn
- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
- Bereitstellung und Betrieb von Software insbesondere des Maklerverwaltungssystems Agentura, dem DokFlow-Analytics-Service sowie weitere Office Produkte zur Nutzung für Internet- oder Intranetangebote des Auftraggebers
- Wartungsarbeiten an den Servern, auf welchen die gemieteten Softwareprodukten installiert sind (umfasst auch: Softwareupdates)
- Sicherung und ggf. auf Anfrage Wiederherstellung von Daten, die mit den gemieteten Softwareprodukten direkt verarbeitet werden
- Auf Anweisung des Auftraggebers Einrichtung von Zugängen für Fremdsysteme und Benutzer zum Zugriff auf die gemieteten Softwareprodukte

2. Dauer des Auftrags

Die Dauer des Auftrags entspricht der Laufzeit der zugrunde liegenden Leistungsvereinbarung.

3. Konkretisierung des Auftragsinhalts

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

4. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezoger Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

☐ Personenstammdaten einschließlich Adressdaten und Einkommensdaten (Vorname, Nachname, Geburtsdatum, Geburtsort, Wohnort, Familienstand, Einkommen, Steuernummern, Geschlecht)

☐ Kommunikationsdaten (z.B. Telefon, E-Mail) und Aufzeichnungen

☐ Benutzerstammdaten (Benutzername, Passwort)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Planungs- und Steuerungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunftdateien, oder aus öffentlichen Verzeichnissen)

☐ Zahlungsdaten (z.B. Kontoverbindung, Kreditkartendaten)

☐ _____

☐ _____

☐ _____

☐ _____

5. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

☐ Kunden

☐ Interessenten

☐ Abonnenten

☐ Beschäftigte i. S. d. § 3 Abs. 11 BDSG

☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner

☐ Benutzer von Internet-Angeboten des Kunden sowie ggf. dessen Kunden

☐ _____

☐ _____

6. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots (vgl. Anlage ...), sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand, die sich aus der zugrundeliegenden Leistungsvereinbarung ergeben. 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. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

7. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

8. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Den Nachweis kann der Auftragnehmer auch durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbringen.

9. Unterauftragsverhältnisse

Der Auftragnehmer gibt bekannt, dass ein Unterauftragsnehmer-Verhältnis mit der ECS Fritz GmbH und der Hetzner Online GmbH besteht, die die Wartung der Server, Datensicherungen, Datenspiegelungen, den Betrieb des Rechenzentrums, Netzwerk-Infrastruktur für den Auftragnehmer übernehmen. Die zuvor genannten Unternehmen haben uns gegenüber ebenfalls entsprechende Erklärung zur Einhaltung des Datenschutzes abgegeben und sind nach ISO27001 zertifiziert.
Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungspflichten verbundene Unternehmen des Auftragnehmers

zur Leistungserfüllung heranzieht bzw. dritte Unternehmen mit Leistungen unterbeauftragt. Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Dies gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

10. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er 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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitäsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSIGrundschutz) erbracht werden.

11. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

12. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes

Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.
Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

13. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen 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.

14. Kostenerstattung

Der Auftraggeber übernimmt alle dem Auftragnehmer entstehenden Kosten als auch die Auftragnehmer eigenen Kosten, die durch Handlungen des Auftraggebers im Rahmen dieser Vertragsvereinbarung entstehen. Insbesondere die Erbringung von Nachweisen, Protokollen als auch die Durchführung von Kontrollen entstehenden Kosten. Der Auftraggeber sollte vor Auftragserteilung diese Kosten im Einzelfall mit dem Auftragnehmer abklären bzw. vereinbaren. Sollte der Auftraggeber keine Kostenvereinbarung für den Einzelfall treffen, so erklärt er stillschweigend mit Auftragserteilung alle Kosten im normalen Umfang zu übernehmen. Der Auftragnehmer kann eine Vorschusszahlung in Höhe von 50 Prozent der zu erwartenden Kosten verlangen und braucht den Auftrag erst dann auszuführen, wenn er die Vorschusszahlung erhalten hat.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlange 1
Technisch-organisatorische Sicherheitsmaßnahmen gemäß § 9 BDSG

Im Folgenden werden die technischen und organisatorischen Maßnahmen geregelt, die bei der durch den Auftragnehmer erbrachten IT-Dienstleistung gemäß Anlage zu § 9 Satz 1 BDSG umzusetzen sind.
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

In den Räumen der ASAsoft GmbH werden keine Daten verarbeitet oder genutzt.
Die Verarbeitung der Daten erfolgt ausschließlich in einem Rechenzentrum in Deutschland, welches nach ISO27001 zertifiziert ist und über folgende Sicherheit verfügt:

1. Zutrittskontrolle
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:
- Einzäunung des Rechenzentrums mit Schutzzaun und Panzerdraht
- 24h/7 Videoüberwachung des Geländes und aller Zutrittstüren
- Zutritt zum Rechenzentrumgelände, Rechenzentrumgebäude, Rechenzentrumräume nur mit elektronischer Pin. Der elektronische Pin erlaubt nur den Zugriff zu vereinbarten Ressourcen. Die zu autorisierende Person wird einmalig bei Pin Übergabe per Ausweiskontrolle verifiziert und eingewiesen in Sicherheits-relevante Belange.
- Das Öffnen des Racks ist nur mit einem Rack-spezifischen Schlüssel / PIN möglich. Jeder berechtigte Mitarbeiter erhält einen eigenen PIN pro Rack. Es ist somit nachvollziehbar und wird protokolliert, welcher Mitarbeiter welches Rack geöffnet hat.
- Eine Schleuse mit 2 Türen soll den Zutritt von Unbefugten ohne Pin verhindern, sollte eine Tür offengelassen worden sein.

2. Zugangskontrolle
Sämtliche DV-Systeme sind mit einem Benutzer/Kennwort geschützt. Die vom Auftragnehmer initial erstellten Kennwörter haben eine Mindestlänge von 8 Zeichen, enthalten Groß- und Kleinbuchstaben und Zahl(en) und entsprechen somit sicheren Kennwörtern. Der Auftragnehmer verwendet für jedes DV-System und jeden Dienst innerhalb eines DV-Systems eigene Benutzer/Kennwörter.

3. Zugriffskontrolle
Tätigkeiten in DV-Systemen sind nur innerhalb der eingeräumten Berechtigungen erlaubt. Im Rahmen der ADV findet kein direkter Zugriff auf personenbezogene Daten durch den Auftragnehmer statt. Falls dies dennoch nötig sein sollte, so erfolgt dies nur durch Kenntnisnahme des Auftraggebers. Berechtigungen werden dokumentiert.

4. Weitergabe Kontrolle
Der Auftragnehmer führt im Rahmen seiner Leistungsvereinbarung eine regelmäßige Datensicherung durch. Die eingesetzte Backupsoftware verschlüsselt die Daten des Auftraggebers am DV-System per sicherer AES 256 Bit Verschlüsselung mit einem persönlichen / Kunden-spezifischen Kennwort und überträgt anschließend die verschlüsselten Daten per sicherer SSL-Verschlüsselung zu den Backupservern des Auftragnehmers. Die Backup-Software führt ein Protokoll über die durchgeführte Datensicherung.

5. Eingabekontrolle
Der Auftragnehmer ist nicht in die Datenverwaltung und –pflege involviert. Sollte dies nötig werden, so ist der Auftragnehmer mit einem spezifischen Benutzer und spezifischen Rechten auszustatten. Der Zugriff ist zu protokollieren.

6. Auftragskontrolle
Der Auftragnehmer erbringt IT-Dienstleistungen nach Umfang des vereinbarten Servicepakets mit standardisiertem klar definiertem Leistungsumfang. Darüberhinausgehende Maßnahmen (technischer / organisatorisch) sind vom Auftraggeber schriftlich zu beauftragen.

7. Verfügbarkeitskontrolle
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch):
- Die Daten werden grundsätzlich nur auf mit RAID 1 (Festplattenspiegelung) oder höher gesicherten Festplatten gespeichert.
- Die Server sind an einer USV angeschlossen.
- Backupserver und DV-System sind 2 getrennte physikalische Einheiten. Die Backupsysteme sind in einem separaten Brandabschnitt untergebracht.
- Die Backupserver verwenden ebenfalls mindestens ein RAID 1 zur Datenspeicherung.
- Alle DV-Systeme sind durch eine Rechenzentrum Firewall mit Einbruchserkennung (IDS) und Einbruchsbekämpfung (IPS) gesichert.
- Alle DV-Systeme verfügen zusätzlich über eine Personal Firewall. Die Firewall Regeln reduzieren den Zugriff auf ausschließlich DV-System spezifisch genutzte Dienste.
- Ein Virenschutz ist optional beim Auftragnehmer erhältlich.

8. Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.
- Software, auf welche Kunden Zugriff haben z.B. zentrale Kundenoberfläche / Backupportal / Monitoringportal, sind grundsätzlich Mandantenfähig mit Rechtemanagement
- Kundendokumente werden in jeweils eigenen Ordnern abgespeichert
- Services des Kunden z.B. Dienstleistungen, Hardware und Software werden in separaten Tabellen in der zentralen Datenbank gespeichert.
- Kennwörter werden aus Sicherheitsgründen entweder gar nicht gespeichert / nur das Initialkennwort im Klartext, welches vom Kunden zu ändern war / gecryptet mit aktuellen Verschlüsselungsverfahren
- Testsysteme arbeiten mit Kopien des Produktivsystems