

# VEREINBARUNG

## zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

**Ihnen, dem Kunden**

*-Auftraggeber-*

und

**smartwork solutions GmbH**

Landsberger Straße 408 - 81241 München

Vertreten durch: Christian Marchsreiter (Geschäftsführer)

*-Auftragnehmer-*

### **Präambel**

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggebers in Berührung kommen können.

## **1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung**

- 1.1 Gegenstand der Auftragsverarbeitung ist im Hauptvertrag beschrieben - im Wesentlichen: die Nutzung des vom Auftragnehmer betriebenen internetbasierten Dienstes **SMASHDOCs** zur kollaborativen Erstellung, Überarbeitung und Produktion von Web-Dokumenten.
- 1.2 Art und Zweck der Auftragsverarbeitung sind im Hauptvertrag beschrieben und umfassen insbesondere die Bereitsstellung und Nutzung von SMASHDOCs sowie Datenarchivierung
- 1.3 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:
  - (a) Name
  - (b) Kontaktdaten, z.B. Telefon, E-Mail
  - (c) Abrechnungsdaten
  - (d) Vertragsstammdaten
  - (e) Protokolldaten
  - (f) Alle anderen personenbezogenen Daten, die in Art. 4 Nr. 1 der DSGVO definiert sind und die vom Kunden im Zuge der Nutzung von SMASHDOCs übermittelt und gespeichert werden
- 1.4 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:
  - (a) Mitarbeiter des Auftraggebers
  - (b) Lieferanten des Auftraggebers
  - (c) Kunden des Auftraggebers
  - (d) Interessenten des Auftraggebers
- 1.5 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben

## **2 Anwendungsbereich und Verantwortlichkeit**

- 2.1 Der Auftragnehmer verarbeitet Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich.
- 2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

### **3 Pflichten des Auftragnehmers**

- 3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichende Verarbeitung verpflichtet ist, weist er – sofern dies rechtlich zulässig ist – den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin.
- 3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die im AVV - Anhang 2: Technisch-organisatorische Maßnahmen des Auftragnehmers beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
- 3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer informiert den Auftraggeber durch eine E-Mail über eine solche Änderung.
- 3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche Betroffener gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.
- 3.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- 3.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- 3.7 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- 3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

- 3.9 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Beschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart.
- 3.10 Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
- 3.11 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

## **4 Pflichten des Auftraggebers**

- 4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- 4.2 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich Auftraggeber und Auftragnehmer hinsichtlich der Verifizierung der Aktivlegitimation bei der Abwehr des Anspruches sich gegenseitig zu unterstützen.
- 4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## **5 Betroffener**

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben des Betroffenen möglich ist.

## **6 Nachweismöglichkeiten**

- 6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in Art 28 DSGVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer, dem Auftraggeber insbesondere Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DSGVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten.
- 6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der

Unterzeichnung einer angemessenen Verschwiegenheitserklärung abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

- 6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.
- 6.4 Für die Unterstützung bei der Durchführung einer Inspektion nach 6.2 oder 6.3 darf der Auftragnehmer eine angemessene Vergütung verlangen, sofern nicht Anlass der Inspektion der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmers war. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Inspektion vom Auftraggeber vorzutragen.

## **7 Subunternehmer (weitere Auftragsverarbeiter)**

- 7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber mit einer Frist von vier Wochen in Textform. Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung des Auftrages beseitigt werden kann, steht dem Auftragnehmer ein Sonderkündigungsrecht zu. Dieses Sonderkündigungsrecht bezieht sich sowohl auf diese Vereinbarung als auch auf den Hauptvertrag. Über die in AVV - Anhang 3: Liste genehmigter Subunternehmer aufgeführten, bei Vertragsschluss bereits bestehenden, Subunternehmer erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggebers besteht für diese Subunternehmer nicht.
- 7.2 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
- 7.3 Auf schriftliche Aufforderung des Auftraggebers hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmer zu erteilen.

## **8 Haftung**

Es wird auf Art. 82 DS-GVO verwiesen. Im Übrigen richtet sich die Haftung aus dieser Vereinbarung nach dem Hauptvertrag.

## **9 Informationspflichten, Schriftformklausel, Rechtswahl**

- 9.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DSGVO liegen.
- 9.2 Folgende Anhänge sind Bestandteil dieser Vereinbarung. Bei Widersprüchen gehen die Regelungen des Textes dieser Vereinbarung den Anhängen vor:
- (a) AVV - Anhang 1: Liste und Kontaktdaten der Ansprechpartner
  - (b) AVV - Anhang 2: Technisch-organisatorische Maßnahmen des Auftragnehmers
  - (c) AVV - Anhang 3: Liste genehmigter Subunternehmer
- 9.3 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 9.4 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- 9.5 Es gilt deutsches Recht.

Datum:

Auftragnehmer:

Auftraggeber:

## AVV - Anhang 1: Liste und Kontaktdaten der Ansprechpartner

Derzeit fungieren **auf Seiten des Auftraggebers** folgende Personen als Weisungsberechtigter bzw. Ansprechpartner für Datenschutzfragen und als dessen Stellvertreter:

Weisungsberechtigter:

- 

Stellvertreter:

- 

Derzeit fungieren **auf Seiten des Auftragnehmers** folgende Personen als Empfangsberechtigter bzw. Ansprechpartner für Datenschutzfragen und als dessen Stellvertreter:

Empfangsberechtigter:

- **Robert Mäckle** (Externer Datenschutzbeauftragter der smartwork solutions GmbH - DataCo GmbH - Siegfriedstraße 8 - 80803 München - +49 (0) 89 7400 45840 - E-Mail: rmaeckle@consulting.dataguard.de)

Stellvertreter:

- **Christian Marchsreiter** (Geschäftsführer der smartwork solutions GmbH)

# **AVV - Anhang 2: Technisch-organisatorische Maßnahmen des Auftragnehmers**

## **1 Pseudonymisierung und Verschlüsselung personenbezogener Daten („pers. Daten“)**

### **1.1 Pseudonymisierung**

Die Verarbeitung von pers. Daten erfolgt in einer Weise, dass diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

### **1.2 Verschlüsselung**

Die eingesetzten Verschlüsselungsmethoden ergeben sich aus den folgenden technischen und organisatorischen Maßnahmen.

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

### **2.1 Zutrittskontrolle**

Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, dass Unbefugten der Zutritt zu Gebäuden und Räumlichkeiten erschwert wird, in denen Datenverarbeitungsanlagen stehen, mit denen pers. Daten verarbeitet werden.

Die Größe der Datenverarbeitungsanlage ist dabei unerheblich. Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Festlegung der berechtigten Personen
- Zutrittsregelungen für betriebsfremde Personen
- Kontrolle der ausgegebenen Zugangsmittel
- Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen
- Abholung betriebsfremder Personen durch Mitarbeiter

### **2.2 Zugangskontrolle**

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte die Datenverarbeitungssysteme, mit denen pers. Daten verarbeitet oder genutzt werden, unberechtigt nutzen können.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Verschlüsselung von Datenträgern
- Regelmäßige Kontrolle der Gültigkeit von Berechtigungen
- Abschottung interner Netze gegen Zugriffe von außen
- Absicherung der Übertragungsleitungen und des Datenstroms

### **2.3 Zugriffskontrolle**

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass nur die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer aufgabenbezogenen Zugriffsberechtigung unterliegenden pers. Daten zugreifen können, und dass pers. Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Für die Geheimhaltung der Zugangsdaten und ggf. deren Weitergabe an Mitarbeiter ist der Auftraggeber selbst verantwortlich.
- Trennung von Test und Produktionsbetrieb
- Einsatz von Verschlüsselungsverfahren

### **2.4 Weitergabekontrolle**

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass pers. Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung pers. Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Mitarbeiter sind auf das Datengeheimnis nach BDSG verpflichtet.
- Die Übertragung der Daten von und zu den Kundenbereichen erfolgt nur SSL-verschlüsselt,
- Für die Einrichtung von Übertragungswegen auf externe Systeme (Datenexport) ist der Auftraggeber selbst verantwortlich.

### **2.5 Eingabekontrolle**

Die Eingabekontrolle soll gewährleisten, dass nachvollzogen werden kann, wer, wann, welche pers. Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt hat.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Die Daten werden vom Auftraggeber selbst eingegeben und verarbeitet.

## **2.6 Trennungskontrolle**

Besonderes Augenmerk sollte darauf gelegt werden, dass gewährleistet ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Daten der Auftraggeber werden physikalisch oder logisch von anderen Daten getrennt gespeichert
- Datensicherung erfolgt ebenfalls physikalisch oder logisch
- "Interne Mandantenfähigkeit"
- Zweckbindung Funktionstrennung /Produktion/ Test)

## **3 Fähigkeit, die Verfügbarkeit der pers. Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Verfügbarkeitskontrolle)**

Die Verfügbarkeitskontrolle soll sicherstellen, dass pers. Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Regelmäßige Datensicherung, Backup-Verfahren
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Virenschutz/ Firewall

## **4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung**

### **4.1 Regelmäßige Überprüfungen der eigenen IT-Systeme**

- Es findet eine regelmäßige Überprüfung und Qualitätssicherung statt, ob sich der Stand der Technik verändert hat und entsprechender Anpassungsbedarf der IT-Systeme besteht.
- Die eingesetzte Hard- und Software wird regelmäßig auf Funktionsfähigkeit überprüft.

- Die Schutzbedarfsklassifizierung für Datenverarbeitungen wird regelmäßig überprüft.

#### **4.2 Regelmäßige Überprüfungen von Subauftragnehmern (Auftragskontrolle)**

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass pers. Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zu diesem Zweck stellt der Auftragnehmer auch sicher, dass der Auftraggeber das Recht hat, auch bei Unterauftragnehmer die hier vereinbarten Überprüfungen vorzunehmen.

Die Umsetzung der folgenden Maßnahmen unterstützt diese Forderung:

- Schriftlicher Vertrag
- Klare Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer
- Definition von Sicherheitsmaßnahmen

## **AVV - Anhang 3: Liste genehmigter Subunternehmer**

Der Auftragnehmer setzt derzeit folgende Unterauftragnehmer ein:

### **Webhosting**

- Hetzner Online GmbH: Industriestr. 25, 91710 Gunzenhausen, Germany