EU-DATENSCHUTZ-GRUNDVERORDNUNG

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

H&S Heilig und Schubert Software AG
Goldschlagstraße 87-89, AT 1150 Wien
tel: +43 (0) 1 21555
fax: +43 (0) 1 21555 200
info@hs-soft.com | www.hs-soft.com

H&S Heilig und Schubert
InformationsManagement GmbH
O´Brien Strasse 3, DE 91126 Schwabach
tel. +49 (0) 9122 87227 0
fax. +49 (0) 9122 87227 399

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

H&S Heilig und Schubert Software AG
Goldschlagstraße 87-89
AT 1150 Wien

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Der Auftraggeber hat den Auftragnehmer durch bestehende Vereinbarungen mit Verarbeitungen personenbezogener Daten beauftragt. Diese bestehenden Vereinbarungen werden durch gegenständliche Zusatzvereinbarung in datenschutzrechtlicher Hinsicht ergänzt.

(2) Vereinbarungsgegenstand ist die Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO. Im Detail handelt es sich um alle notwendigen und vereinbarten Maßnahmen zur Implementierung und Bereitstellung der Softwareprodukte des Auftragnehmers inklusive Wartung und Pflege von Softwareprodukten des Auftragnehmers wie Fernbetreuung, Fehlerdiagnosen, Wartungs- oder Servicetätigkeiten. Es kann nicht ausgeschlossen werden, dass der Auftragnehmer im Zuge der Implementierung sowie bei Programmierungs-, Wartungs- und Pflegearbeiten personenbezogene Daten beim Auftraggeber einsehen bzw. lesen kann und muss.

Im Zuge der Erfüllung des Supportvertrages wird der Auftragnehmer Zugriff auf sämtliche Datenkategorien von sämtlichen Betroffenen erhalten, die der Auftraggeber mit den Softwareprodukten des Auftragnehmers verarbeitet.

2. DAUER DER VEREINBARUNG

Die Vereinbarung beginnt und endet mit dem Supportvertrag. Hiervon unberührt sind die nachvertraglichen Pflichten des Auftragnehmers, insbesondere die sich aus Art 28 DSGVO ergebenden Verpflichtungen bei Beendigung von Auftragsverarbeitungsverträgen.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dass der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

(10) Leistungen des Auftragnehmers, die dieser für den Auftraggeber im Zusammenhang mit den Verpflichtungen des Auftraggebers aus der DSGVO erbringt, sind mit dem jeweils aktuellen Stundensatz des Auftragnehmers zu entlohnen, sofern diese nicht ausdrücklich im Supportvertrag genannt sind, und eine Vereinbarung über deren Honorierung besteht.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

5. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuzuziehen:

H&S Heilig und Schubert InformationsManagement GmbH
DE-91126 Schwabach
UID-Nr.: DE213309477, AG Nürnberg HRB 19707

Weitere Sub- Auftragsverarbeiter

Der Auftragnehmer kann weitere Sub-Auftragsverarbeiter hinzuziehen. Er hat den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Für den Auftraggeber Ort, Datum	Für den Auftragnehmer Ort, Datum
_____ Unterschrift Name und Funktion	_____ Unterschrift Name und Funktion

6. ANLAGE ./1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

VERTRAULICHKEIT

- **Zutrittskontrolle:**

Benutzung eines automatisierten Verarbeitungssystems bei dem die Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden Verbindungen Zugang haben.	Der Zutritt zu der Remoteverbindung des Kunden erfolgt über eine Berechtigung (Es besteht eine Passwort-Policy), oder der Zugang ist nur durch und während einer Überprüfung durch den Auftraggeber möglich. In diesem Fall ist eine Freischaltung durch den Auftraggeber ist bei jedem Verbindungsaufbau notwendig.
Eingänge zum Firmengelände	Die Eingänge sind versperrt. Nur Mitarbeiter erhalten einen Schlüssel.

- **Zugangskontrolle**:

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)	Der Zugang kann folgenderweise erfolgen: a) auf einem virtuellen PC eingerichtet und es sind nur diejenigen Personen zutritts- bzw. zugriffsberechtigt, die dazu von der Leitung des Auftragnehmers berechtigt wurden. b) der Zugang erfolgt on demand mit Team Viewer oder GotoMeeting am PC des Supporter – zu jeder Session muss der Auftraggeber aktiv zustimmen.
Benutzeridentifikation und Authentifizierung: Kennwortverfahren	Die Systeme sind durch eine Benutzer-Passwort-Authentifikation gesichert. Das Passwort unterliegt diversen Sicherheitsregeln (u.a. Sonderzeichen, Mindestlänge) und muss alle 90 Tage geändert werden. Nach wiederholter Falscheingabe wird der Account zudem für 30min gesperrt.
Automatische Sperrung	Nach 15min Inaktivität wird ein Benutzer automatisch ausgeloggt.
Einrichtung eines Benutzerstammsatzes pro User	Benutzerkonten werden mit, für den Nutzer passenden, Rollen versehen um sicherzustellen, dass nur Zugriff auf Bereiche besteht, die für dessen Tätigkeit notwendig sind.
Virenschutz / Firewall	Unsere lokale Infrastruktur ist durch eine Firewall von äußeren Zugriffen geschützt.

- **Zugriffskontrolle**:

Benutzung eines automatisierten Verarbeitungssystems, bei dem Berechtigte ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle)	Der Auftraggeber regelt die Passwort-Policy für die befugten Mitarbeiter des Auftragnehmers beim Zugriff auf sein System. und diese ist den Befugten auch bekannt.

INTEGRITÄT

- **Weitergabekontrolle**:

Personenbezogene Daten können bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden Der Auftragnehmer überprüft und stellt fest, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Die Verarbeitung der Daten beschränkt sich auf die Einsichtnahme auf den Systemen des Auftraggebers mittels Remote-Zugang. Eine permanente Speicherung der Daten beim Auttragnehmer erfolgt nicht und ist auch nicht möglich. In Ausnahmefällen erfolgt in ausdrücklicher Abstimmung mit dem Auftraggeber eine Übermittelung und Speicherung der Daten. Diese können zuvor anonymisiert werden und werden im Anschluss gelöscht.
Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung: Verschlüsselung / Tunnelverbindung	Der Zugriff von außen auf das H&S Netz erfolgt über gesicherte VPN-Tunnel.
Protokollierung	VPN-Traffic wird protokolliert und regelmäßig überprüft.

- **Eingabekontrolle**:

Nachträgliche Überprüfung und Kontrolle, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle)	Der Auftraggeber wird dafür Sorge tragen, dass der Remotezugriff aufgezeichnet und auf seinen Systemen protokoliert wird. Der Auftragnehmer wird den Auftraggeber bei der Einrichtung entsprechender Aufzeichnungs- und Protokollierungssoftware unterstützen.

VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle:**

Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Die Verarbeitung der Daten beschränkt sich auf das Abfragen, somit sind die Daten prinzipiell gegen zufällige Zerstörung oder Verlust geschützt. Besteht die Möglichkeit einer Veränderung wird auf die Daten im Rahmen eines 4 Augen Prinzips zugegriffen.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
- Incident-Response-Management

ENDE DOKUMENT