Verpflichtungserklärung zur Auftragsverarbeitung nach Art. 28 Abs. 9 DSGVO

SELSA Intelligence AG für Internet, neue Medien und E-Commerce
Grabenstraße 92
8010 Graz
als „**Auftragsverarbeiter**"

verpflichtet sich gegenüber dem **Verantwortlichen** (= Auftraggeber = Kunde) wie folgt:

1 Vertragsgegenstand

a. Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich Versicherungsvergleich und –beratung für Endverbraucher auf Grundlage eines schriftlichen Vertrags. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

b. Die Laufzeit dieser Verpflichtungserklärung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

2 Art der verarbeiteten Daten, Kreis der Betroffenen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die hier näher spezifizierten personenbezogenen Daten.

Folgende Datenkategorien werden uA. verarbeitet:
Personendaten allgemein, Anschriftsdaten, Kommunikationsdaten, Legitimationsdaten, Berufs- und Arbeitgeberdaten, Daten von Familien- und Haushaltsangehörigen, Personendaten körperlich, Personendaten Gewohnheiten, Versicherungsvertragsdaten allgemein, Versicherungsdaten des zu versichernden Risikos, Bankverbindungsdaten, Ausbildungsdaten, Bonitätsdaten, gescannte Dokumente und Bilddateien.

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:
Kunden, Interessenten, Versicherungsgesellschaften-Ansprechpartner.

3 Weisungsrecht

a. Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der

Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

b. Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen im Rahmen des zugrundeliegenden Vertrages zwischen Auftraggeber und Auftragnehmer berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

c. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4 Schutzmaßnahmen des Auftragsverarbeiters

a. Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

b. Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen.

   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

c. Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden Mitarbeitende genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.
   Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung des Hauptvertrages oder des Beschäftigungsverhältnisses zwischen den Mitarbeitenden und dem Auftragsverarbeiter bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5 Informationspflichten des Auftragsverarbeiters

a. Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält.

b. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich in Schriftform informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde.

c. Über wesentliche Änderung der Sicherheitsmaßnahmen nach Punkt 4 hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

6 Kontrollrechte des Verantwortlichen

a. Der Verantwortliche kann sich jederzeit vor der Aufnahme der Datenverarbeitung und auch danach von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er sich eventuell vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen.

b. Ist dies nicht möglich, kann er die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

   Der Auftragsverarbeiter verpflichtet sich in diesem Fall, dem Verantwortlichen auf dessen mündliche oder schriftliche Aufforderung innerhalb einer angemessenen Frist jene Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

c. Der Auftragsverarbeiter weist dem Verantwortlichen die Verpflichtung der Mitarbeiter nach Punkt 4 c auf Verlangen nach.

7 Einsatz von Subunternehmern

a. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt. Er setzt den Verantwortlichen hiervon unverzüglich in Kenntnis.

b. Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Verpflichtungserklärung ebenso zu verpflichten. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

c. Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste.

8 Anfragen und Rechte Betroffener

a. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

b. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbständig, sondern verweist den Betroffenen unverzüglich an den Verantwortlichen und wartet dessen Weisungen ab.

9 Haftung

a. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter alleine der Verantwortliche gegenüber dem Betroffenen verantwortlich.

b. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

10 Beendigung des Hauptvertrags

a. Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Republik Österreich eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen.

b. Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Verpflichtungserklärung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

11 Schlussbestimmungen

a. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

b. Diese Vereinbarung unterliegt österreichischem Recht. Ausschließlicher Gerichtsstand ist Graz.

c. Der Auftragsverarbeiter ist berechtigt, jederzeit rechtskonforme Änderungen an dieser Verpflichtungserklärung vorzunehmen. Sollte er eine Änderung vornehmen (müssen), verpflichtet er sich, die jeweils letztgültige Version dieser Verpflichtungserklärung unaufgefordert dem Verantwortlichen in elektronischer Form zur Verfügung zu stellen.

Graz, im Mai 2020

SELSA Intelligence AG für Internet, neue Medien und E-Commerce

SELSA
SELSA INTELLIGENCE • AKTIENGESELLSCHAFT
A-8010 GRAZ - GRABENSTRASSE 92
TEL.: +43-316-33 83 70 - FAX +43-316-33 8370-2133
WWW.CHEGG.NET - OFFICE@CHEGG.NET

Mag. Thomas Lang, CEO

Anlagen
Anlage 1 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters bzw. Subunternehmers
Anlage 2 – Subunternehmer

Anlage 1 – Technisch-organisatorische Maßnahmen

Zutrittskontrolle:
a) Rechenzentrum: 24/7 Zugang zum Rechenzentrum (SysUP-Housing) erfolgt nur mit personalisierter Zutrittskontrolle via Zutrittskarte und Rackschlüssel; nur autorisierte Personen haben Zutritt zum Rechenzentrum; Videoüberwachungsanlage ist vorhanden; Serverracks sind versperrt.
b) Betriebsgebäude: Alarmanlage; Schließsystem mit Codesperre; Sicherheitsschlösser;

Auftragskontrolle:
Der Auftragsverarbeiter nimmt keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen vor. Die Dienstleister, denen sich der Auftragsverarbeiter bedient, werden von diesem unter Anlage strenger Kriterien ausgewählt und kontrolliert. Die getroffenen Sicherheitsmaßnahmen werden im Vorhinein geprüft. Die Mitarbeiter des Auftragsverarbeiters werden durch Vereinbarung zum Datenschutz verpflichtet.

Zugangskontrolle:
Der Zugriff auf die Systeme erfolgt per Secure Shell und ist nur mit gültigen Benutzerdaten möglich. Die Berechtigungen am System (Ordnerberechtigungen, etc.) wurden nach besten Wissen so hoch wie möglich gesetzt. Richtlinien für die Vergabe von administrativen Benutzerrechten sind daher nicht notwendig. Auf den Systemen werden administrative Arbeiten nur von SysUP- oder von SELSA AG-Mitarbeitern durchgeführt.

Weitergabekontrolle:
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, Virtual Private Networks (VPN) und elektronische Signatur.

Zugriffskontrolle:
Die Zugriffe auf das Server-System werden protokolliert. Für jeden Benutzer ist ein eigenes Systemkonto auf den Servern vorhanden. Ausgeführte Befehle werden über Syslog (Paranoia Log) mitprotokolliert und können jederzeit abgerufen werden.
Der Remote-Zugriff für die Administration der Systeme erfolgt ausschließlich über eine verschlüsselte Secure Shell Verbindung.
Die Anzahl der Administratoren ist auf das Notwendigste reduziert. Schutz vor unbefugter Systembenutzung erfolgt grundsätzlich durch Kennwörter (einschließlich entsprechender Policy) in Verbindung mit automatischen Sperrmechanismen; es bestehen Passwortrichtlinien inkl. Passwortlänge;
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich.
Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert gespeichert (=Pseudonymisierung)

Eingabekontrolle:
Sofern vom Auftraggeber gewünscht, kann durch Einrichtung individueller Zugänge zum System mit Benutzername und Passwort protokolliert werden, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind;

Verfügbarkeitskontrolle:
Die Verfügbarkeit der Serversysteme wurde über einen Clustersystem (DRBD) mit 2 Servern auf ein Maximum erhöht. Zusätzlich verfügt das Rechenzentrum über eine USV-Anlage, ein Dieselaggregat, eine Brandmelde- und Löschanlage (Löschgas FM200 nicht korrosiv, nicht elektrisch leitend) inkl. Brandfrüherkennungssystem (VESDA). Eine redundante Klimaanlage gewährleistet Ausfallsicherheit und eine konstante Temperatur. Die Anbindung an das Internet wird über eine direkte redundante Anbindung

über den Provider UPC-Austria realisiert. Die Infrastrukturkomponenten von SysUP sind ebenfalls durchgängig redundant ausgeführt.
Zur Datensicherung wird ein tägliches Backup (1x Full, 6x inkrementell) ausgeführt. Die Backup-Daten werden auf einen dedizierten Backupserver im gleichen Rechenzentrum übertragen. Auf allen Systemen (wo technisch möglich) werden 1x pro Monat aktuelle Sicherheitsupdates installiert. Systemlogs werden proaktiv kontrolliert.
Veränderungen von Systemdateien werden automatisch an SysUP per Email (Tripwire, ViperDB) übermittelt. Auf den Loadbalancer-Serversystemen kommt zusätzlich eine Iptables Firewall für den Schutz von außen zum Einsatz.

Backup von Dateidaten: 7 Tage; Datenbanken 14 Tage; Logfiles bzw. Systemlogfiles (Authentifizierung, Kernel, User, Cron, Debug): 7 Tage; Maillogfiles: 7 Tage; MySQL (Datenbank): 7 Tage; Apache (Webzugriff): 365 Tage (52 Wochen); Zusätzliche Applikationslogs (Apache): 1000 Tage

Trennungsgebot:
Trennung von Produktiv- und Echtsystem; Festlegung von Datenbankrechten; logische Mandantentrennung (softwareseitig) in Teilbereichen der Applikation;

Anlage 2 – Auflistung der Subunternehmer

Subunternehmer	Land	Funktion
Fa. SysUP OG	Österreich	Serverhousing und Serverhosting