Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Vereinbarung zwischen _____ **und**
(Kundennummer)

_____ Zenker Office AG
(Name, Firma)

_____
(Bezeichnung)

_____ Happinger Straße 71
(Straße, Hausnummer)

_____ 83026 Rosenheim
(PLZ, Ort)

(Verantwortlicher, nachfolgend „Auftraggeber“ genannt) *(Auftragsverarbeiter, nachfolgend „Auftragsnehmer“ genannt)*

---

§1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus den bestehenden Verträgen und deren Leistungsvereinbarungen.
(2) Die Laufzeit dieses Auftrages entspricht der Laufzeit der Leistungsvereinbarungen.
(3) Die Kündigung der Leistungsvereinbarung bedingt automatisch die Kündigung dieses Auftrags. Eine gesonderte Kündigung dieses Auftrags ist in diesem Falle nicht nötig.

§2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in den Leistungsvereinbarungen konkret beschrieben.
(2) Folgende personenbezogene Daten erheben wir im Zusammenhang mit der Leistungsvereinbarung von Ihnen:
- Personenstammdaten,
- Kommunikationsdaten (z.B. Telefon, E-Mail),
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse),
- Kundenhistorie,
- Vertragsabrechnungs- und Zahlungsdaten,
- Ablesedaten,
- Prüfdaten,
- Planungs- und Steuerungsdaten sowie Verbindungsdaten.

(3) Durch die Verarbeitung betroffen sind folgende Personengruppen:
- Kunden,
- Interessenten,
- Beschäftigte beim Kunden,
- Lieferanten / Dienstleister,
- Ansprechpartner,
- Planungs- und Steuerungsdaten sowie
- Verbindungsdaten.

(4) Die vertraglich vereinbarte Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der EU oder des EWR statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur dann erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

§3 Technisch-organisatorische Maßnahmen

(1) Gem. Art 28 Abs. 3 lit. c, 32 EU-DSGVO hat der Auftragnehmer:
„die Sicherheit, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen.“

Wir haben unsere technisch-organisatorischen Maßnahmen ausführlich in Anlage 1 dargestellt.

(2) 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.

§4 Berichtigung, Einschränkung und Löschung von Daten

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. Der Auftragnehmer kann für diese Unterstützungsleistungen eine angemessene Vergütung verlangen.

§5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich gesetzliche Pflichten gemäß Art. 23 bis 33 EU-DSGVO; d.h. er gewährleistet insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt:
Unser Datenschutzbeauftragter ist:

Andreas Stürzl
Interaktiv Stürzl & Licht GbR
Haidenholzstr. 33
83071 Stephanskirchen

Telefon 08036 / 90 80 – 520
E-Mail dsb@interaktiv-edv.de
Internet www.interaktiv-edv.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29. 32 Abs. 4 EU-DSGVO:
Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers einschließlich der in diesem Vertrag eingeräumten Befugnisse verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c. 32 EU-DSGVO:
Einzelheiten hierzu finden Sie in Anlage 1.

(4) Zusammenarbeit mit der Aufsichtsbehörde bei Anfrage zur Erfüllung von deren Aufgaben.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

§6 Unterauftragsverhältnisse

(1) Als Untervertragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- oder Transportleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf sich bei der Ausübung seiner vertraglich vereinbarten Aufgaben anderer Dienstleister bedienen, insbesondere Auftragsverarbeiter nach Art. 28 DSGVO.

§7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen 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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§8 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.
- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten, Verletzungsereignissen ermöglichen die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, auf Wunsch des Auftraggebers und dessen Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) 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. Die Vertragspartner sind berechtigt diese Vereinbarung jederzeit zu ändern, sofern sich dies aus gesetzlichen oder datenschutzbehördlichen Anforderungen zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO oder aus Änderungen in der Rechtsprechung ergibt. Änderungen müssen schriftlich zugesandt werden. Sie gelten als angenommen und werden Vertragsbestandteil, wenn ihnen nicht innerhalb von 6 Wochen widersprochen wird.

(4) Diese Vereinbarung beginnt mit Wirksamwerden der EU-DSGVO am 25.05.2018.

Anlage - Technisch-organisatorische Maßnahmen

Der Auftraggeber bestätigt mit seiner Unterschrift ein Exemplar des Vertrags erhalten zu haben und der Vereinbarung zur Auftragsverarbeitung zuzustimmen.

_____, _____
Ort ***Datum***

_____
Stempel, Unterschrift (Auftraggeber)

Rosenheim, 16.05.2018

zenker OFFICE
ZENKER OFFICE AG
Happinger Str. 71 • 83026 Rosenheim
Tel. + 49(0) 8031 / 61699-0 • Fax -11

_____
Stempel, Unterschrift (Auftragnehmer)

Sofern Sie eine/n Datenschutzbeauftragte/n benannt haben, benötigen wir die Kontaktdaten. Wir sind gem. Art. 30 Abs. 2 lit. a EU-DSGVO verpflichtet, diese in unser Verzeichnis von Verarbeitungstätigkeiten als Auftrags-verarbeiter aufzunehmen. (Nur ausfüllen, falls ein/e Datenschutzbeauftragte/r benannt wurde.)

_____
(Name)

_____
(Telefon)

_____
(Straße)

_____
(E-Mail)

_____
(PLZ, Ort)

Anlage 1 -Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

Zutrittskontrolle

- Die Datenverarbeitungssysteme befinden sich in den Räumlichkeiten der Zenker Office AG und sind in abgeschlossenen Serverschränken und Gehäusen untergebracht.
- Nur einzelne, auf den Datenschutz verpflichtete und registrierte Personen haben im Rahmen ihrer dort auszuübenden Tätigkeit Zutritt zu den Serverschränken und Gehäusen.
- Die Schlüsselvergabe erfolgt ausschließlich an berechtigte Personen.
- Ein Empfang ist vorhanden / Kameraüberwachung im Gebäude besteht.

Zugangskontrolle

Es wurde ein Zugangskonzept erstellt. Nur die autorisierten und authentifizierten Personen können auf die Systeme zugreifen. Die Anmeldung an den Systemen wird protokolliert.

- Ein Kennwortverfahren ist gewährleistet
- Eine automatische Sperrung erfolgt mittels Bordmitteln, Kennwort für Freischaltung
- Zugriffe auf das Netzwerk der Zenker Office AG aus dem Internet erfolgen nur über SSL
- Kritische Bereiche wie das CRM System des Auftragnehmers verfügen über keine Verbindungen zum Internet, die Arbeitsplatzrechner sind gegen die Entnahme von Daten aus diesen Systemen geschützt.

Zugriffskontrolle

Die Erstvergabe und die Verwaltung von Zugriffscodes obliegen ausschließlich dem Verantwortungsbereich des Auftragnehmers. Ein Berechtigungskonzept ist vorhanden. Soweit technisch möglich und wirtschaftlich vertretbar, werden geeignete Verschlüsselungstechnologien eingesetzt.

- Die Zugriffskontrolle erfolgt mittels eines Berechtigungskonzeptes.
- Realisierung differenzierter Berechtigungen durch Benutzerprofile.
- Kritische Bereiche wie das CRM System des Auftragnehmers verfügen über keine Verbindungen zum Internet, die Arbeitsplatzrechner sind gegen die Entnahme von Daten aus diesen Systemen geschützt.
- Datenträger werden ordnungsgemäß vernichtet.

Trennungskontrolle

Die Programme sind für die getrennte Verarbeitung der Daten ausgelegt. Dieses wird durch ein detailliertes Berechtigungskonzept zusätzlich garantiert. Die Daten werden entsprechend der Ordnungsbegriffe und Kundennummer ausgewertet.

- Funktionstrennung durch produktive EDV-Systeme, Testsysteme und Vorführsysteme.

Pseudonymisierung

(Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO) Die Zuordnung personenbezogener Daten erfolgt erst nach Datenübertragung (Internet) bei uns im Backend, eine Pseudonymisierung erfolgt nicht.

- Berechtigungskonzept über Login-Vorgang
- Datenbankrechte durch Login-Konzept der Datenbank

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

Weitergabekontrolle

Nur autorisierte Personen haben Zugriff auf die Daten während des Transports. Beim elektronischen Datenaustausch besteht das Sicherungssystem aus vielschichtigen und komplexen Prüfungen. Sicherheitsvorkehrungen in den Betriebsräumen gewährleisten, dass ein unbefugtes Entfernen von Datenträgern aus den Sicherheitsbereichen verhindert wird. Entsorgungsgut mit schutzwürdigem Inhalt wird durch eine hausinterne Shredderanlage, bzw. durch ein nach § 52 KrW-lAbfG zertifiziertes Unternehmen, unter Beachtung des Vier-Augen-Prinzips nach einer hohen Sicherheitsstufe vernichtet.

ZENKER OFFICE AG
Happinger Straße 71
D-83026 Rosenheim
HRB 22169 Traunstein
USt-IDNr. DE131203125

Tel. +49 (0) 8031 • 6 16 99-0
Fax +49 (0) 8031 • 6 16 99-11
info@zenker-office.de
www.zenker-office.de
U.d.PBS-Ehrenkodex

Vorstand
Walter Zenker sen. (Vorsitzender)
Dipl.-Kfm.(FH) Wolfgang F. Zenker
Vorsitzender Aufsichtsrat
Klaus Kemper

Sparkasse Rosenheim-Bad Aibling: IBAN DE64 7115 0000 0000 0022 53 BIC BYLADEM1ROS
VR-Bank Rosenheim-Chiemsee eG: IBAN DE57 7116 0000 0100 0112 66 BIC GENODEF1VRR

Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete physikalische Techniken und Verschlüsselungstechnologien eingesetzt.

- Die Zugriffskontrolle erfolgt mittels eines Berechtigungskonzeptes.
- Die Transportsicherung erfolgt mittels https.

Eingabekontrolle

Ein mehrstufiges Protokollierungs - und Auditingverfahren gewährleistet, dass Änderungshistorien verursachergerecht - dort, wo erforderlich – fortgeschrieben werden. Diese Daten werden entsprechend der gesetzlich vorgeschriebenen Aufbewahrungsfristen vorgehalten.

- Protokollierungs- und Protokollauswertungssysteme sind gewährleistet.
- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement und die im Qualitätsmanagement des Auftragnehmers dokumentieren betrieblichen Prozesse.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

Verfügbarkeitskontrolle

Die Daten werden gemäß des Backup-Konzeptes redundant und nach Stand der Technik gesichert und geeignet aufbewahrt (Sicherheit, Zugriff). Geeignete Verlustsicherungsmaßnahmen sind etabliert. Zusätzlich sind unsere Rechensysteme mittels eines USV-Systems (unterbrechungsfreie Stromversorgung) gegen Stromausfall abgesichert.

- Backup-Verfahren wird angewendet (Vollbackup und differenzielle Backups).
- Festplatten werden durch gängige Verfahren gespiegelt.
- eine USV (unterbrechungsfreie Stromversorgung) ist gegeben.
- eine getrennte Aufbewahrung ist realisiert.
- Virenschutz und Firewall sind vorhanden.

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust ist u.a. gewährleistet durch das Backup-Konzept, unterbrechungsfreie Stromversorgung (USV), Virenschutz und Firewall.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Ant 25 Abs. 1 EUvDSGVO)

- Backup-Konzept wird angewendet (Vollbackup und differenzielle Backups)
- Datenschutz-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)
- Auftragskontrolle

ZENKER OFFICE AG
Happinger Straße 71
D-83026 Rosenheim
HRB 22169 Traunstein
USt-IDNr. DE131203125

Tel. +49 (0) 8031 • 6 16 99-0
Fax +49 (0) 8031 • 6 16 99-11
info@zenker-office.de
www.zenker-office.de
U.d.PBS-Ehrenkodex

Vorstand
Walter Zenker sen. (Vorsitzender)
Dipl.-Kfm.(FH) Wolfgang F. Zenker
Vorsitzender Aufsichtsrat
Klaus Kemper

Sparkasse Rosenheim-Bad Aibling: IBAN DE64 7115 0000 0000 0022 53 BIC BYLADEM1ROS
VR-Bank Rosenheim-Chiemsee eG: IBAN DE57 7116 0000 0100 0112 66 BIC GENODEF1VRR