Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Artikel 28 Datenschutzgrundverordnung (DSGVO)

zwischen

- im folgenden Auftraggeber genannt -

und

KALORIMETA GmbH
Heidenkampsweg 40
20097 Hamburg

- nachfolgend Auftragnehmer genannt -

§ 1 Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet gem. dem geschlossenen Vertrag personenbezogene Daten im Auftrag des Auftraggebers. Die Laufzeit dieser Vereinbarung entspricht der des Dienstleistungsvertrages.

Der Auftrag umfasst folgenden Umfang und Auftragszweck:

- Erheben der Verbrauchswerte von Heizung, Warm- sowie Kaltwasser und etwaiger Betriebskosten,
- Berechnung der jeweiligen Verbrauchskosten für die einzelnen Nutzer
- Erstellung von Heiz- und Betriebskostenabrechnungen auf Nutzerebene
- Vermietung und Montage messtechnischer Einrichtung

Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union bzw. in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenkategorien:

- Personenstammdaten (Name, Vorname, Adresse, Geburtsdatum)
- Wohnungsstammdaten (Fläche, Belegenheit)
- Kommunikationsdaten (Telefon- und Telefaxnummer, E-Mail Adresse)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Abrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten oder aus öffentlichen Verzeichnissen)

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Kunden
- Eigentümer
- Lieferanten
- Handelsvertreter
- Behörden
- Mitarbeiter
- Mieter
- Dienstleister
- Ansprechpartner

Diese Vereinbarung tritt mit Unterzeichnung beider Parteien in Kraft und gilt, solange die geschlossenen Service-/Mietverträge Gültigkeit haben.

§ 2 Technisch-organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich, seine innerbetriebliche Organisation entsprechend dem Auftrag so auszugestalten, dass sie den jeweils geltenden Datenschutzanforderungen gerecht wird.

Der Auftragnehmer hat die Sicherheit gem. Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 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 DSGVO zu berücksichtigen.

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.

§ 3 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.

§ 4 Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Artikel 28 DSGVO folgende Pflichten:

(1) Schriftliche Bestellung – soweit gem. Art. 37 DSGVO - vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausüben kann. Kontaktdaten: Karin Krutzinna, KALORIMETA GmbH, Heidenkampsweg 40, 20097 Hamburg, datenschutz@kalo.de
(2) Die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen Art. 32 DSGVO.

(4) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt.

(5) 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.

(6) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzaudit, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) vorlegen.

(7) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(8) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht diese Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lt. a DSGVO).

§ 5 Unterauftragsverhältnisse

Unterauftragsverhältnisse sind Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Der Auftragnehmer kann zur Vertragsdurchführung unter Wahrung seiner unter Punkt 4 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen.
- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichen falls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

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,

Reinigungskräfte oder Prüfer. 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.

§ 6 Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die 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 vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrages stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nach Art. 28 DSGVO überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen 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) erbracht werden. Das Recht auf Stichprobenkontrollen vor Ort steht dem Auftraggeber auch nach Vorlage o. g. Nachweise zu.

§ 7 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

Es ist bekannt, dass 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 Betriebsablaufes, bei Verdacht auf sonstige Verletzung 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.

§ 8 Weisungsbefugnis des Aufraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. 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 Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail 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 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. Der Auftraggeber stellt den Auftragnehmer von Geldbußen und Schadensersatzansprüchen Dritter frei.

§ 9 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. Gleiches gilt für Test- und Ausschussmaterial. 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.

§ 10 Haftung

Der Auftragnehmer haftet für eigenverursachte oder durch Erfüllungsgehilfen verursachte Schäden, die aus der Verletzung einer wesentlichen Vertragspflicht bestehen. Es wird auf Art. 82 DSGVO verwiesen.

§ 11 Sonstiges

1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
2. Für Nebenabreden ist die Schriftform erforderlich.
3. Die Einrede des Zurückbehaltungsrechts i. S. von § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
4. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

, Hamburg,

_____ _____

- Auftraggeber - - Auftragnehmer -

Anlage

Allgemeine technische und organisatorische Maßnahmen (TOM's)

1. Zutrittskontrolle

Durch nachstehende Maßnahmen verwehren wir Unbefugten den Zutritt zu den Geschäftsräumen:

- Zutrittskontrollsystem (Codekarte)
- Schlüsselberechtigungssystem für sensible Bereiche (Datenverarbeitung, Personaldaten)
- Türsicherung über verschiedene Schließkreise
- Schlüsselregelung (Ausgabe von Schlüsseln)
- Überwachungseinrichtung (Alarmanlage, Kameras)
- Sicherheitsverglasung
- Protokollierung Besuche Externer (Besucherliste und -ausweise)
- Gesonderte Sicherung des Rechenzentrums
- Serverräume gesondert gesichert, Zutritt nur durch autorisierte Personen
- Videoüberwachung der Zugänge

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme wird verhindert. Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Kennwortverfahren
- Automatische Sperrung
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Festplattenverschlüsselung bei mobilen Rechnern
- Firewall
- Einsatz von Anti-Viren-Software

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden verhindert. Bedarfsorientierte Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Kennwortverfahren
- Datenträgerverwaltung
- Protokollierung Systemzugriffe
- Einsatz von Dienstleistern zur Aktenvernichtung
- ordnungsgemäße Vernichtung von Datenträgern

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten werden geregelt. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselung/Tunnelverbindung (VPN=Virtual Private Network)
- Beim physischen Transport: Sichere Transportbehälter/-verpackungen
- Regelung für den Transport von Datenträgern
- Verschlüsselung von USB Sticks
- eigene Cloudlösung
- Papierunterlagen mit personenbezogenen Daten werden von Spezialfirmen entsorgt
- Datenträger werden qualifiziert vernichtet, Festplatten gelöscht

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, gewährleistet:

- Protokollierungs- und Protokollauswertungssystematiken
- Benutzeridentifikation
- Archivierung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung wird durch folgende Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer gewährleistet:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
- Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten werden gegen zufällige Zerstörung oder Verlust mittels Maßnahmen zur Datensicherung (physikalisch/logisch) geschützt:

- Backup-Verfahren
- Spiegeln von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung von Datensicherungen
- Externe Lagerung von Datensicherungen
- Virenschutz / Firewall
- Notfallplan
- Feuerlöscher und Brandmeldeanlage
- Externes Ausweichrechenzentrum für Notfälle
- Überspannungsschutz
- Klimaanlage in Serverräumen

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt verarbeitet. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Interne Mandantenfähigkeit
- Funktionstrennung Produktion/Test mit getrennten Datenbanken sowie aktuellen Verschlüsselungsverfahren

9. Datenschutzmanagement

- Es wurde eine Datenschutzbeauftragte bestellt
- Alle Mitarbeiter wurden auf die Einhaltung datenschutzrechtlicher Vorschriften sowie auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse verpflichtet
- Die Mitarbeiter werden durch regelmäßige Schulungen und andere Informationen zum Datenschutzrecht für das Thema sensibilisiert

10. Maßnahmen zur Belastbarkeit der IT-Systeme

- Regelmäßige Penetrationstests der eigenen IT-Systeme

11. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM’s zur Gewährleistung der Sicherheit der Verarbeitung

- Interne Verhaltensrichtlinien
- Regelmäßige Überprüfung der TOM’s
- Meldeprozess für Datenschutzverletzungen
- Durchführung von Datenschutzfolgeabschätzungen soweit erforderlich
- Dokumente werden in unserem sicheren Kundenportal zur Verfügung gestellt