

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Dieser Auftragsverarbeitungsvertrag (nachfolgend „Vertrag“ oder „AVV“) wird geschlossen zwischen

Verantwortlicher („Auftraggeber“)	Der Kunde, der über die Plattform eee-cad.de ein Projekt beauftragt, mit den bei der Buchung angegebenen Firmen- und Kontaktdaten.
Auftragsverarbeiter („Auftragnehmer“)	K&S Energy GmbH, Am Wiesengrund 25, 63075 Offenbach am Main, eingetragen im Handelsregister des Amtsgerichts Offenbach am Main unter HRB 58395, vertreten durch den Geschäftsführer Dipl.-Ing. Jörg Schäfer, E-Mail: info@eee-cad.de, Betreiberin der Plattform eee-cad.de – nachfolgend „Anbieter“.

Der Auftraggeber und der Anbieter werden nachfolgend gemeinsam „Parteien“ genannt. Durch aktives Anhaken der Zustimmungs-Checkbox im Buchungsprozess kommt dieser Vertrag verbindlich zustande.

§ 1 Gegenstand und Grundlage

(1) Der Anbieter betreibt die Online-Plattform eee-cad.de und erstellt für den Auftraggeber digitale CAD-Modelle zum Zweck der Energieberatung. Der Anbieter erbringt selbst keine Energieberatungsleistungen. Grundlage sind die vom Auftraggeber bereitgestellten Gebäudeunterlagen (z. B. Pläne, PDFs, Fotos).

(2) Im Rahmen dieser Leistungserbringung verarbeitet der Anbieter personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Dieser AVV konkretisiert die datenschutzrechtlichen Pflichten der Parteien gemäß Art. 28 DSGVO. Er gilt für alle Verarbeitungstätigkeiten, die der Anbieter im Zusammenhang mit dem Hauptvertrag (Nutzung der Plattform / Projektbeauftragung) durchführt.

(3) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, der Anbieter ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO. Gegenstand, Art, Zweck, Datenkategorien und Kategorien betroffener Personen ergeben sich aus Anlage 1.

(4) Nicht Gegenstand dieses Vertrags ist die Verarbeitung der Vertrags-, Rechnungs- und Zahlungsdaten des Auftraggebers selbst. Diese verarbeitet der Anbieter als eigenständig Verantwortlicher auf Grundlage seiner Datenschutzerklärung; die Zahlungsabwicklung erfolgt über einen Zahlungsdienstleister außerhalb dieses Auftragsverhältnisses.

§ 2 Weisungsrecht des Auftraggebers

- (1) Der Anbieter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist gesetzlich zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Anbieter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- (2) Die bei der Projektbuchung getroffenen Festlegungen sowie die Anlagen dieses Vertrags gelten als Erstweisung. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform (z. B. per E-Mail).
- (3) Der Anbieter informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Umsetzung der betreffenden Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

§ 3 Pflichten des Anbieters (Auftragsverarbeiter)

- (1) Der Anbieter verpflichtet sich, personenbezogene Daten vertraulich zu behandeln und ausschließlich im Rahmen der Auftragsdurchführung zu verarbeiten.
- (2) Der Anbieter stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO) und über die einschlägigen Datenschutzbestimmungen unterrichtet wurden. Die Vertraulichkeitspflicht besteht auch nach Beendigung des Auftrags fort.
- (3) Der Anbieter trifft die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 2 und hält diese während der Vertragslaufzeit auf dem aktuellen Stand der Technik.
- (4) Der Anbieter benennt auf Anfrage einen Ansprechpartner für Datenschutzfragen. Sofern gesetzlich erforderlich, wird ein Datenschutzbeauftragter benannt.
- (5) Der Anbieter unterstützt den Auftraggeber bei der Erfüllung der Rechte betroffener Personen (Art. 12–23 DSGVO) sowie bei den Pflichten nach Art. 32–36 DSGVO im Rahmen des Zumutbaren. Für Unterstützungsleistungen, die nicht auf einem vom Anbieter zu vertretenden Verstoß beruhen, kann der Anbieter eine angemessene Vergütung verlangen; er teilt die voraussichtlichen Kosten vorab mit.
- (6) Der Anbieter berichtet, löscht oder sperrt die im Auftrag verarbeiteten Daten ausschließlich nach Weisung des Auftraggebers, soweit keine gesetzliche Aufbewahrungspflicht besteht.

§ 4 Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit einem Antrag auf Ausübung ihrer Rechte unmittelbar an den Anbieter, leitet dieser den Antrag unverzüglich an den Auftraggeber weiter.
- (2) Der Anbieter beantwortet solche Anträge nicht selbst, es sei denn, er wurde vom Auftraggeber hierzu ausdrücklich ermächtigt. Bei der Bearbeitung befolgt der Anbieter die Weisungen des Auftraggebers.

- (3) Der Anbieter haftet nicht dafür, wenn ein Antrag der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 5 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Anbieter dokumentiert die getroffenen Sicherheitsmaßnahmen in Anlage 2. Diese gewährleisten ein dem Risiko angemessenes Schutzniveau, insbesondere Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme.

(2) Änderungen der Maßnahmen sind zulässig, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Anbieter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt.

(2) Der Anbieter informiert den Auftraggeber über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) vorab in Textform. Der Auftraggeber kann einem Wechsel innerhalb von 14 Tagen aus wichtigem, datenschutzrechtlichem Grund widersprechen.

(3) Der Anbieter verpflichtet Unterauftragsverarbeiter vertraglich auf ein Datenschutzniveau, das den Anforderungen dieses Vertrags entspricht (Art. 28 Abs. 4 DSGVO), und stellt durch regelmäßige Überprüfungen sicher, dass diese die technischen und organisatorischen Maßnahmen einhalten. Als Unterauftragsverarbeitung gelten nicht Nebenleistungen Dritter (z. B. Telekommunikation, Wartung), die der Anbieter angemessen absichert.

§ 7 Meldung von Datenschutzverletzungen

(1) Der Anbieter meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, in Textform.

(2) Die Meldung enthält mindestens: Art der Verletzung, betroffene Datenkategorien, wahrscheinliche Folgen und die ergriffenen bzw. vorgeschlagenen Gegenmaßnahmen. Der Anbieter unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO).

§ 8 Kontroll- und Nachweisrechte

(1) Der Anbieter stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.

(2) Der Auftraggeber ist berechtigt, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen – vorrangig durch Einholung geeigneter Nachweise (z. B. Zertifikate, Testate, Selbstauskunft). Vor-Ort-Kontrollen sind mit angemessener Vorankündigung (mind. 14 Tage) und während der Geschäftszeiten möglich, ohne den Betriebsablauf unverhältnismäßig zu stören.

(3) Für Informations- und Unterstützungsleistungen im Rahmen von Kontrollen kann der Anbieter eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines vom

Anbieter zu vertretenden Verstoßes erforderlich wurde.

§ 9 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Datenübermittlung an den Anbieter sowie der Verarbeitung allein verantwortlich (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO).
- (2) Der Auftraggeber informiert den Anbieter unverzüglich und vollständig, wenn er bei der Auftragsdurchführung Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellt.
- (3) Der Auftraggeber löscht vor Vertragsende diejenigen personenbezogenen Daten, die er eigenverantwortlich in den Diensten des Anbieters gespeichert hat, soweit sie nicht der Löschung nach § 11 unterliegen.
- (4) Auf Anforderung des Anbieters benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

§ 10 Datenverarbeitung außerhalb der EU / des EWR

- (1) Die Verarbeitung findet grundsätzlich innerhalb der EU bzw. des EWR statt. Eine Verarbeitung in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44–49 DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss oder Standardvertragsklauseln der EU-Kommission).
- (2) Ein in Anlage 3 aufgeführter Unterauftragsverarbeiter (SKIY31 GmbH) verarbeitet im Rahmen der Leistungserbringung personenbezogene Projektdaten teilweise aus der Ukraine (Drittland ohne Angemessenheitsbeschluss). Zur Absicherung dieser Übermittlung hat der Anbieter mit dem Unterauftragsverarbeiter EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914) abgeschlossen.
- (3) Der Anbieter ergreift ergänzende Schutzmaßnahmen (insbesondere Verschlüsselung bei Übertragung und Speicherung, strenge Zugriffskontrolle, Datenminimierung) und hat die Zulässigkeit der Übermittlung im Rahmen einer Transfer-Folgenabschätzung (Transfer Impact Assessment) geprüft. Zugänge in der Entwicklung nutzen ausschließlich Test-/Dummy-Daten.

§ 11 Löschung und Rückgabe nach Vertragsende

- (1) Nach Abschluss der Leistungserbringung löscht der Anbieter alle im Auftrag verarbeiteten Daten oder gibt sie nach Wahl des Auftraggebers zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart.
- (2) Vorbehaltlich abweichender Weisung erfolgt die Löschung spätestens 60 Tage nach Projektabschluss bzw. Vertragsende. Die Löschung wird auf Verlangen in Textform bestätigt. Von der Pflicht ausgenommen sind gesetzlich aufbewahrungspflichtige Unterlagen (z. B. steuer- und handelsrechtliche Belege).

§ 12 Verantwortlichkeit und Haftung

- (1) Die Verantwortlichkeit für die Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen liegt beim Auftraggeber.
- (2) Die Haftung der Parteien im Außenverhältnis richtet sich nach Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für den von ihr zu vertretenden Anteil. Etwaige Haftungsbeschränkungen des Hauptvertrags gelten entsprechend, soweit gesetzlich zulässig.

§ 13 Vertragsdauer, Änderungen und Schlussbestimmungen

- (1) Dieser Vertrag gilt für die Dauer des Hauptvertrags bzw. der Projektbeauftragung. Findet eine Verarbeitung noch nach Vertragsende statt, gelten diese Regelungen bis zum tatsächlichen Ende der Verarbeitung fort. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt; ein wichtiger Grund liegt insbesondere bei schwerwiegenden Verstößen gegen datenschutzrechtliche Bestimmungen vor.
- (2) Der Anbieter kann diese Vereinbarung mit angemessener Ankündigungsfrist ändern, insbesondere bei wesentlichen rechtlichen Änderungen. Er weist den Auftraggeber auf die Bedeutung der Änderung hin und räumt ihm eine angemessene Widerspruchsfrist ein; widerspricht der Auftraggeber nicht fristgerecht, gilt die Änderung als angenommen. Im Fall eines Widerspruchs steht dem Anbieter ein außerordentliches Kündigungsrecht zu.
- (3) Werden Daten des Auftraggebers beim Anbieter durch Pfändung, Beschlagnahme, ein Insolvenz- oder Vergleichsverfahren oder sonstige Maßnahmen Dritter gefährdet, informiert der Anbieter den Auftraggeber unverzüglich und weist alle Beteiligten darauf hin, dass die Datenhoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.
- (4) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Regelungen dieses AVV in datenschutzrechtlichen Fragen vor. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (5) Ausschließlicher Gerichtsstand für Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist – vorbehaltlich eines ausschließlich gesetzlichen Gerichtsstands – der Sitz des Anbieters. Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand	Erstellung digitaler CAD-Modelle aus vom Auftraggeber bereitgestellten Gebäudeunterlagen zum Zweck der Energieberatung; es werden keine Energieberatungsleistungen erbracht.
Art der Verarbeitung	Erheben, Speichern, Auslesen, Auswerten, Umwandeln, Übermitteln (Ergebnisrückgabe) und Löschen der bereitgestellten Daten.
Zweck	Erstellung der beauftragten CAD-Modelle.
Art der Daten	In hochgeladenen Unterlagen enthaltene Daten: Namen und Anschriften von Gebäudeeigentümern / Bewohnern, Kontaktdaten, Grundstücks- und Gebäudedaten, ggf. Fotos, sowie Kontaktdaten von Ansprechpartnern des Auftraggebers.

Kategorien Betroffener	Kunden und Ansprechpartner des Auftraggebers, Gebäudeeigentümer, Mieter/Bewohner, Mitarbeitende des Auftraggebers.
Dauer	Für die Dauer der Projektbeauftragung; Löschung gemäß § 11 dieses Vertrags.
Löschfristen	Projektdaten: spätestens 60 Tage nach Projektabschluss. Sicherungskopien (Backups) und Protokolldaten (Logfiles): spätestens 90 Tage nach Projektabschluss. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Zutrittskontrolle: gesicherte Geschäftsräume, Zugangsbeschränkung für Unbefugte.
- Zugangskontrolle: individuelle Benutzerkonten, starke Passwörter, Zwei-Faktor-Authentifizierung.
- Zugriffskontrolle: rollenbasierte Berechtigungen, Zugriff nur für berechtigte Mitarbeitende, keine öffentlichen Dateilinks.
- Trennungskontrolle: mandantengetrennte, projektbezogene Ablage der Kundendaten.

Integrität

- Weitergabekontrolle: verschlüsselte Übertragung (TLS/HTTPS) beim Up- und Download.
- Eingabekontrolle: Protokollierung von Zugriffen und Änderungen (Logging).

Verfügbarkeit & Belastbarkeit

- Regelmäßige Backups, Schutz vor Datenverlust.
- Verschlüsselte Speicherung (at rest) bei EU-basiertem Hosting/Dateiablage.
- Schutzmaßnahmen gegen Schadsoftware und unbefugten Zugriff.

Datenminimierung & Drittland-Schutz

- Weitergabe an den Unterauftragsverarbeiter (Modellierung) auf das für die Leistung erforderliche Maß beschränkt.
- Verschlüsselung bei Übertragung und Speicherung; strenge, rollenbasierte Zugriffskontrolle.
- Drittland-Übermittlung auf Grundlage von EU-Standardvertragsklauseln zzgl. ergänzender Maßnahmen (siehe § 10); Entwicklungszugänge nur mit Test-/Dummy-Daten.

Verfahren zur Überprüfung

- Auftragskontrolle: vertragliche Bindung eingesetzter Dienstleister.
- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen; definiertes Löschkonzept.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Aufgeführt sind die vom Anbieter (K&S Energy GmbH) direkt beauftragten Unterauftragsverarbeiter. Der Zahlungsdienstleister ist nicht gelistet, da die Zahlungsdaten vom Anbieter als eigenständig Verantwortlichem verarbeitet werden (siehe Datenschutzerklärung).

Dienstleister	Zweck	Sitz / Verarbeitungsort	Garantien bei Drittlandtransfer
1&1 IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Webhosting / Speicherung Projektdateien	Deutschland	Speicherung in DE. IONOS kann gem. eigenem AVV (Anhang 2) Unterauftragsverarbeiter in Drittländern (u. a. USA, z. B. CDN/Malware-Schutz) einsetzen – abgesichert durch EU-Standardvertragsklauseln.
SKIY31 GmbH, Weinstraße 5, 67146 Deidesheim	Technische Entwicklung und Wartung der Plattform sowie technische Verarbeitung projektbezogener Daten	Sitz: Deutschland; Verarbeitung personenbezogener Projektdateien teilweise aus der Ukraine (Drittland). Entwicklung nur mit Test-/Dummy- Daten.	EU-Standardvertragsklauseln zzgl. ergänzender Schutzmaßnahmen (Art. 46 DSGVO); Transfer Impact Assessment durchgeführt.
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	E-Mail- und Kollaborationsdienste (Microsoft 365 / Outlook)	Irland (EU); Verarbeitung teils in Drittländern (USA)	EU-US Data Privacy Framework zzgl. EU-Standardvertragsklauseln (Microsoft Data Protection Addendum).