Vertrag über die Auftragsverarbeitung

Zwischen

Name/Firma*	
Straße/Nr.*	
PLZ/Ort *	

nachstehend **„Auftraggeber“** genannt

und

enco energie control GmbH

Rombacher Hütte 2

44795 Bochum

nachstehend **„Auftragnehmer“** genannt

nachstehend beide zusammen auch die **„Parteien“**

und jeder für sich auch die **„Partei“** genannt

* Pflichtfelder

Präambel

Der Auftraggeber ist

- Eigentümer einer oder mehrerer Immobilien oder
- als Hausverwalter namens und in Vollmacht der von ihm vertretenen Eigentümer tätig,
- hat den Auftragnehmer mit der Erbringung von Messdienstleistungen oder Rauchwarnmelder-Services sowie gegebenenfalls damit verbundenen Dienstleistungen beauftragt (im Folgenden „Leistungsvereinbarung“ genannt) und wird dies gegebenenfalls auch in Zukunft tun.
- Dieser Vertrag (im Folgenden auch „Auftragsvereinbarung“ genannt) enthält den schriftlichen Auftrag zur Auftragsverarbeitung im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (DS-GVO) an den Auftragnehmer und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.
- Alle vor dieser Vereinbarung geschlossenen Vereinbarungen zur Datenverarbeitung werden durch diese Vereinbarung ersetzt.

1. Erfasste Leistungsvereinbarungen und Dauer des Auftrags

1.1. Erfasste Leistungsvereinbarungen

Die Auftragsvereinbarung erfasst sämtliche bereits abgeschlossenen sowie die zukünftigen Leistungsvereinbarungen, die Auftragnehmer und Eigentümer (ggf. vertreten durch den Auftraggeber) schließen werden.

1.2. Auftragsvereinbarung Dauer

Die Dauer der Auftragslaufzeit entspricht der Laufzeit der jeweils zwischen Auftragnehmer und den Eigentümern (ggf. vertreten durch den Auftraggeber) geschlossenen Leistungsvereinbarungen.

1.3. Stellung und Rechte der Verantwortlichen im Sinne der DS-GVO und der Hausverwaltung

1.3.1. Verantwortlicher im Sinne der DS-GVO für die unter dieser Auftragsvereinbarung verarbeiteten personenbezogenen Daten ist immer der Eigentümer/sind immer die Eigentümer der von dieser Auftragsvereinbarung umfassten Immobilie(n).

1.3.2. Schließt eine Hausverwaltung diese Auftragsvereinbarung im Namen eines Eigentümers oder mehrerer Eigentümer ab, dann gilt Folgendes:

(1) Die vom Auftraggeber vertretenen Eigentümer ergeben sich aus den vorstehend in Bezug genommenen Leistungsvereinbarungen. Schließt der Auftraggeber während der Laufzeit dieser Auftragsvereinbarung weitere Leistungsvereinbarungen (sowohl für bereits bei Abschluss dieser Vereinbarung erfasste als auch für neue Eigentümer), dann unterfallen diese ebenfalls dieser Auftragsvereinbarung.

(2) Die Hausverwaltung hat die Geltendmachung der Rechte der Eigentümer nach dieser Auftragsvereinbarung zu koordinieren und nimmt diese, soweit ihr möglich, im Namen des Eigentümers selbst gegenüber dem Auftragnehmer wahr; daher verweist diese Auftragsvereinbarung bei der Zuweisung von Rechten und Pflichten auf den Auftraggeber und nicht auf die Eigentümer. Die Stellung der vertretenen Eigentümer als Verantwortliche und Vertragspartner des

Auftragnehmers und die Ausübung ihrer Rechte nach den Leistungsvereinbarungen oder dieser Auftragsvereinbarung bleiben hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

2.1. Gegenstand, Art und Zweck der vorgesehenen Verarbeitung von Daten

2.1.1. Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind konkret beschrieben in den Leistungsvereinbarungen.

2.1.2. Darüber hinaus erfolgt die Verarbeitung zu Zwecken der Erkennung und Behebung von Fehlern und Qualitätsproblemen.

2.1.3. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO) und durch Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

2.2. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten von Mieter/innen und Nutzer/innen, sowie Ansprechpartner des Kunden
- Kommunikationsdaten (z.B. Telefon, E-Mail) von Mieter/innen und Nutzer/innen, sowie Ansprechpartner des Kunden
- Verbrauchsdaten (Heizung, Warmwasser, Kaltwasser, Strom, Gerätenummern) von Mieter/innen und Nutzer/innen
- Protokoll- und Messdaten (z.B. notwendige Zustandsinformationen von Geräten)
- Sonstige Abrechnungsdaten von Mieter/innen und Nutzer/innen

2.3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Mieter/innen der Eigentümer und Nutzer/innen der Immobilien, sowie die Ansprechpartner des Kunden

3. Technisch-organisatorische Maßnahmen

3.1. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 wie in der Anlage zu dieser Auftragsvereinbarung näher spezifiziert. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche

3.2. Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

3.3. Der Auftragnehmer kontrolliert die technischen und organisatorischen Maßnahmen regelmäßig auf ihre Angemessenheit und entwickelt diese unter Berücksichtigung des technischen Fortschritts weiter. 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. Die jeweils aktuelle TOM-Liste wird auf Anfrage zur Verfügung gestellt.

4. Berichtigung, Einschränkung und Löschung von Daten; Geltendmachung Rechte Betroffener

4.1. Die Löschung der Daten erfolgt unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen, wenn sie für die Erbringung der Leistungen nicht mehr erforderlich sind; für Ablesedaten, Funk- und Messdaten beträgt die Löschungsfrist 10 Jahre nach Erhebung. Abweichende Einzelweisungen sind zulässig, wenn sie nicht den gesetzlichen Aufbewahrungsfristen der enco energie control GmbH widersprechen kann hierzu eine angemessene Vergütung verlangen.

4.2. Der Auftragnehmer hat den Auftraggeber mit geeigneten und zumutbaren Maßnahmen zu unterstützen, wenn betroffene Personen ihre datenschutzrechtlichen Rechte nach Art. 15 ff. DS-GVO wahrnehmen und der Auftraggeber dies nicht selbst in zumutbarer Weise tun kann. Wendet eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Die Verantwortung für die Erfüllung der geltend gemachten Rechte gegenüber den betroffenen Personen obliegt dem Eigentümer.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers unter Datenschutzerklärung – enco energie control GmbH

- Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Unterstützung des Auftraggebers im angemessenen Umfang bei einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsvereinbarung.

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

6. Unterauftragsverhältnisse

6.1. Unterauftragnehmer im Sinne dieser Regelung sind Erbringer solche Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung der Leistungsvereinbarung beziehen. Nicht hierzu gehören Erbringer von Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice, die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes auch bei Nebenleistungen angemessene Maßnahmen zu ergreifen.

6.2. Der Auftraggeber stimmt zu, dass der Auftragnehmer Unterauftragnehmer einsetzt.

6.2.1. Bei Abschluss dieser Auftragsvereinbarung sind dies die unter folgendem Link aufgeführten Unterauftragnehmer: https://portal.enco.de/gas/ua/r/hkp300

6.2.2. Einspruchsrecht:

(3) Über die Hinzuziehung neuer oder die Ersetzung bestehender Unterauftragnehmer informiert der Auftragnehmer den Auftraggeber 30 Tage vorab per E-Mail (wenn bekannt) oder Post und er aktualisiert die Dienstleisterliste unter: https://portal.enco.de/gas/ua/r/hkp300

(4) Ein Einspruch kann nur innerhalb der vorstehenden Frist von 30 Tagen eingelegt werden, vorausgesetzt die vereinbarten Kriterien nach Ziffer 6.4 sind nicht eingehalten oder es besteht berechtigter Anlass zur Sorge, dass eine nicht datenschutzkonforme Verarbeitung beim Unterauftragnehmer droht. Bleibt ein Einspruch des Auftraggebers innerhalb der vorgenannten Frist aus, gilt die beabsichtigte Änderung in Bezug auf den betreffenden Unterauftragnehmer als akzeptiert. Maßgeblich ist der Zeitpunkt des Zugangs der Einspruchserklärung.

6.3. Sofern der Auftraggeber der Verarbeitung von personenbezogenen Daten beim Unterauftragnehmer in berechtigter Weise widerspricht, hat der Auftragnehmer ein Sonderkündigungsrecht bezüglich der Leistungsvereinbarung(en) oder Teilen davon. Der Vergütungsanspruch des Auftragnehmers bleibt für Leistungen, die bereits zum Zeitpunkt der Sonderkündigung erbracht worden sind, unberührt.

6.4. Der Auftragnehmer hat vertraglich sicherzustellen, dass die Bestimmungen dieser Auftragsvereinbarung inhaltlich auch mit dem Unterauftragnehmer vereinbart werden. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen.

7. Kontrollrechte des Auftraggebers

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

7.2. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; durch die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); oder durch eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.3. Der Auftraggeber hat zudem das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen. 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.

7.4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer angemessenen Ersatz der hierfür nachweislich angefallenen erforderlichen Aufwendungen geltend machen.

8. Unterstützungsleistungen

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 33 bis 36 der DS-GVO genannten Pflichten, d.h. Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.

- die Verpflichtung, Verletzungen personenbezogener Daten des Auftragnehmers unverzüglich an den Auftraggeber zu melden,
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht bei Verletzungen personenbezogener Daten des Auftragnehmers gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
- die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung,
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2. Für Unterstützungsleistungen im Rahmen von Datenschutz-Folgenabschätzungen sowie hierbei erforderlichen Konsultationen mit der Aufsichtsbehörde, kann der Auftragnehmer angemessenen Ersatz der hierfür nachweislich angefallenen erforderlichen Aufwendungen verlangen.

9. Weisungsbefugnis des Auftraggebers

9.1. Dieser Vertrag sowie die Leistungsvereinbarung enthalten die abschließenden Regelungen zur Verarbeitung personenbezogener Daten. Soweit Einzelweisungen hiernach oder nach Gesetz zulässig sind, hat der Auftraggeber mündliche Weisungen unverzüglich mindestens in Textform zu bestätigen.

9.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Überzeugung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1. Nach Aufforderung durch den Auftraggeber hat der Auftragnehmer die personenbezogenen Daten dem Auftraggeber auszuhändigen oder datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ziffer 10.2 bleibt unberührt.

10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Information über neue Unterauftragnehmer per Kundenportal

Sie können die Liste unserer Unterauftragnehmer über den Link zur Dienstleisterliste einsehen.
https://portal.enco.de/gas/ua/r/hkp300

_____, den _____ [Ort], den [Datum]

Dieser Auftragsverarbeitungsvertrag ist auch ohne handschriftliche oder elektronische Unterschrift gültig. Die Zustimmung erfolgt durch Abschluss des Hauptvertrags.

_____ _____

Auftraggeber (Signatur) Auftragnehmer (Signatur)

Thomas Puszicha (Geschäftsführer)

_____

Auftraggeber (Name) *Die Vertragsannahme durch den Auftragnehmer ist nur gültig, sofern keine Änderungen am Vertragsinhalt vorgenommen wurden.

Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

  Alarmanlage, Zugang zum Gebäude nur mit Chip außerhalb der Geschäftszeiten, Empfang, Innerhalb der Büroräume Zutritt nur mittels Transponder, Besucherraum, Abgeschlossener Serverraum (Zugang nur für berechtigte Personen)

- Zugangskontrolle
  Kein unbefugter Zugang zu Datenverarbeitungssystemen:

  Authentifizierung mittels individueller Benutzerkennungen und persönlicher Passwörter, Einsatz von Multi-Faktor-Authentifizierung, VPN-Verbindungen, Umsetzung von Richtlinien zur Passwortkomplexität und Passwortlänge, Sofortige Sperrung bzw. Löschung von Benutzerkonten bei Austritt oder Rollenwechsel, Protokollierung und Überwachung von Anmeldeversuchen, Automatische Bildschirmsperre nach definierter Inaktivitätszeit, Beschränkung privilegierter Zugänge auf einen definierten Personenkreis, Nutzung administrativer Konten ausschließlich für administrative Tätigkeiten, Trennung von Standard- und Administratorkonten

- Zugriffskontrolle

  Kein unbefugter Zugriff auf Daten:

  Vergabe von Zugriffsrechten nach dem Need-to-know-Prinzip, Rollen- und aufgabenbasierte Berechtigungsvergabe (Role-Based Access Control), Technische Beschränkung des Zugriffs auf sensible Datenbestände, Freigabeprozesse für die Vergabe, Änderung und Entziehung von Berechtigungen, Beschränkung des Zugriffs auf bestimmte Anwendungen, Systeme oder Datenbereiche, Technische Trennung von Test- und Produktivumgebungen

- Trennungskontrolle

  Technische Trennung von Kunden-, Mitarbeiter- und Lieferantendaten, Dokumentation der Verarbeitungszwecke, Sensibilisierung der Mitarbeitenden hinsichtlich Zweckbindung und Datenminimierung; Funktionstrennung

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Transportverschlüsselung (z. B. TLS/HTTPS) bei der Datenübertragung, VPN-gesicherte Kommunikationsverbindungen, Verschlüsselung von Datenträgern und mobilen Endgeräten, Einschränkung externer Speichermedien (USB-Kontrolle), Regelungen zur Übermittlung personenbezogener Daten, Definition zulässiger Kommunikationskanäle, Vertraulichkeitsvereinbarungen mit Mitarbeitenden und Dienstleistern

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch: Festlegung von Benutzerberechtigungen (Profile); Differenzierte Benutzerberechtigungen; Teilzugriff auf Daten bzw. Funktionen; Organisatorische Festlegung von Eingabezuständigkeiten; Verpflichtung auf das Datengeheimnis

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

  Regelmäßige Datensicherungen (Backups), Automatisierte Backup- und Wiederherstellungsverfahren, Einsatz unterbrechungsfreier Stromversorgungen (USV), Schutz vor Schadsoftware durch Virenschutz, Firewall, Notfallmanagement, dokumentierter Notfallplan, Definierte Vertretungsregelungen, Wartungs- und Servicekonzepte

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Mandantentrennung zwischen verschiedenen Auftraggebern, Einschränkung administrativer Zugriffe auf autorisierte Personen, Verschlüsselte Datenübertragung zwischen Auftraggeber und Auftragsverarbeiter, Abschluss von Auftragsverarbeitungsverträgen (AVV), Durchführung von Audits und Kontrollen, Regelungen zur Meldung von Datenschutzvorfällen, Schulungen zum Datenschutz und zur Informationssicherheit