

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen

dem Auftraggeber

- *nachstehend Verantwortlicher genannt* -

und

Beyer GmbH & Co. KG IBIA

Merscheider Busch 23

42699 Solingen

- *nachstehend Auftragsverarbeiter genannt* -

1. Gegenstand und Dauer des Auftrages

(1) Gegenstand

Der Gegenstand dieser Vereinbarung zur Auftragsverarbeitung (nachfolgend „Vereinbarung“ genannt) und die Kontaktdaten des Verantwortlichen ergeben sich aus dem jeweiligen Auftrag bzw. Vertrag auf den hier verwiesen wird (nachfolgend „Auftrag“ genannt).

(2) Dauer

Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Auftrages.

2. Konkretisierung des Inhalts der Vereinbarung

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen betrifft im Wesentlichen

- die Montage und die (Fern-)Ablesung sowie Wartung der zur verbrauchsabhängigen Heizkostenabrechnung benötigten Erfassungsgeräte (Heizkostenverteiler, Wärme- und Wasserzähler)
- die Montage und die (Fern-)Wartung von Rauchwarnmeldern
- die Probenahme für Legionellenprüfungen
- die Erstellung der Heiz- und Hausnebenkostenabrechnung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat 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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten

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

- Personenstammdaten
- Kommunikationsdaten
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Mieter-/Wohnungseigentümerdaten (z.B. Name, Anschrift, Umlageschlüssel, Verbrauchsdaten)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden

- Interessenten
- Servicepartner (Ableser, Monteure)
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Mieter, Wohnungseigentümer

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter setzt die technischen und organisatorischen Maßnahmen in der Anlage 1 um. Die dokumentierten Maßnahmen sind Grundlage der Vereinbarung. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 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 (Einzelheiten in Anlage 1).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Rechte von betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte nach Kapitel III der Datenschutzgrundverordnung (DSGVO). Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrages gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gem. Art. 38 und 39 DSGVO ausübt. Für den Auftragsverarbeiter ist als Beauftragte(r) bestellt:

Herr Arndt Halbach
GINDAT GmbH
Wetterauer Straße 6

42897 Remscheid

E-Mail: datenschutz@beyeribia.de

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Umsetzung und Einhaltung aller für diese Vereinbarung erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anlage 1).

d) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

f) Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

g) Der Auftragsverarbeiter 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieser Vereinbarung.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, 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 Auftragsverarbeiter ist jedoch verpflichtet, zur

Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

- (2) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter auf Grundlage der hier allgemein erteilten schriftlichen Einwilligung einsetzen. Der Verantwortliche stimmt der Beauftragung der in Anlage 2 bezeichneten Unterauftragnehmer zu, soweit: mit diesen eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

Die Auslagerung auf weitere Unterauftragnehmer oder deren Wechsel ist zulässig, wenn:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- (3) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
 - (4) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
 - (5) Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Hauptauftragsverarbeiters (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

7. Kontrollrechte des Verantwortlichen

- (1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mit einem Vorlauf von mindestens vier Wochen anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Die vom Verantwortlichen dafür eingesetzten Personen müssen sich gegenüber dem Auftragsverarbeiter zur Geheimhaltung verpflichten. Die Geheimhaltungsverpflichtung muss hohen Sicherheitsanforderungen genügen. Die eingesetzten Personen dürfen in keiner Beziehung zu einem Wettbewerber des Auftragsverarbeiters stehen.
- (2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter

verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

- (3) Der Nachweis solcher Maßnahmen kann erfolgen durch:
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
 - aktuelle Testate, Berichte oder Berichtsanzüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, DIN-ISO 27001).

8. Mitteilung bei Verstößen des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen 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. Hierzu gehören u.a.
 - 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
 - b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
 - c) die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
 - d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgeabschätzung
 - e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- (2) Der Auftragsverarbeiter ist berechtigt, für Unterstützungsleistungen eine angemessene Vergütung nach Zeit- und Materialaufwand zu verlangen, sofern sie nicht in der Leistungsvereinbarung enthalten und die auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind sowie sich ausschließlich in der Erfüllung der sich unmittelbar aus der DSGVO bzw. dem BDSG ergebenden Pflichten des Auftragsverarbeiters bestehen. Vorbehaltlich einer anderen Vereinbarung mit dem Verantwortlichen gilt für die Vergütung unserer Fachkräfte ein Stundensatz i.H.v. 150,00 EUR zzgl. der jeweils gültigen Mehrwertsteuer. Materialaufwand und Reisekosten rechnet der Auftragsverarbeiter gegenüber dem Verantwortlichen in der tatsächlich entstandenen Höhe ab.

9. Weisungsbefugnis des Verantwortlichen

- (1) Der Auftragsverarbeiter verarbeitet die perso-

nenbezogenen Daten des Verantwortlichen ausschließlich entsprechend der Weisung des Verantwortlichen. Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

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

10. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Auftrags – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhandigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Anforderung zu bestätigen.
- (3) Von den Lösch- und Rückgabepflichten sind solche Daten ausgenommen, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht (z.B. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren).

Solingen, den 29.12.2025

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Anlage 1 - Technisch-organisatorische Maßnahmen

1. Gewährleistung der Vertraulichkeit der Systeme und Dienste,

die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen. Nur berechtigte Personen dürfen von schützenswerten Daten Kenntnis nehmen (Art. 32 Abs. 1 Lit. b DSGVO).

Zutrittskontrollmaßnahmen

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

- Physische und organisatorische Sicherheitsmaßnahmen (Empfang zur Registrierung) sind für nicht-öffentliche Bereiche implementiert
- Besucher der Firmenzentrale dürfen nicht-öffentliche Bereiche nur in Begleitung betreten
- Physische Zugangsbeschränkung für Unbefugte zu dem Rechenzentrum sowie den Servern in den Niederlassungen
- Berechtigungsprüfung des Zutritts zu sensiblen Bereichen des Rechenzentrums mit Abgleich von autorisierten Personen
- Führen eines Schlüsselverzeichnisses für die Firmenzentrale
- Implementierte Einbruchschutzmaßnahmen (Videoüberwachung)
- Protokollierung der Besuche in der Firmenzentrale

Zugangskontrollmaßnahmen

Schutz vor unbefugter Systembenutzung

- Der Zugang zu Systemen ist nur mit individuellen Benutzernamen und Kennwörtern möglich
- Definierte Anforderungen an Mindestlänge und Komplexität der Kennwörter
- Automatische Bildschirm- und Rechnersperre bei Nichtbenutzung
- Der Zugang zu den Systemen ist nur einem definierten Kreis von Zugangsberechtigten möglich
- Es erfolgt eine Protokollierung der Benutzeranmeldung und der jeweiligen Zeitpunkte

Zugriffskontrollmaßnahmen

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, verändert oder entfernt werden können.

- Zugriff nach Berechtigungskonzept je nach Aufgabenstellung
- Personenbezogene Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden
- Eine Verwendung fortlaufend aktualisierter Virenschutzsoftware ist technisch sichergestellt
- Eingehender E-Mail-Verkehr wird durch ein zentrales Virenschutz- und Spamfiltersystem auf Viren und Spam überprüft
- Schutz der IT-Infrastruktur durch Firewalls
- Passwortschutz

Maßnahmen zur Trennungskontrolle

damit zu unterschiedlichen Zwecken - insbesondere für unterschiedliche Kunden - erhobene bzw. zu verarbeitende Daten getrennt voneinander verarbeitet werden.

- Logische Trennung der Server
- Trennung von Produktiv- und der Test- und Entwicklungsumgebung

2. Maßnahmen zur Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in der Weise, dass die Daten in den unterschiedlichen Systemen nicht ohne Hinzuziehung zusätzlicher Informationen einer spezifischen betroffenen Person zugeordnet werden können, sofern dies möglich und sinnvoll ist (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO).

3. Gewährleistung der Integrität der Systeme und Daten

(Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen zur Weitergabekontrolle

- Verschlüsselung/Nutzung von VPN-Tunneln bei Übertragung
- SSL-Verschlüsselung bei Web-Access
- Regelung des Systemkommunikationsverkehrs (Zentrale Firewall, exklusive WAN-Verbindung mit Zugriffskontrollen), Protokollierung (User-Authentifizierung, Zeitpunkt)

Maßnahmen zur Eingabekontrolle

- Protokollierung
- Berechtigungskonzept

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

- Personenbezogene Daten sind ständig verfügbar und durch regelmäßige Datensicherungen gegen zufällige Zerstörung und Verlust geschützt
- Datensicherungskonzept (tägliche Backups)
- Aufbewahrungsmodalitäten der Backups (Safe)
- Besonders geschützte Serverräume
- Brandschutzvorrichtungen in der Firmenzentrale und den Niederlassungen
- Redundante Stromzuführung

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-/Datensicherheitskonzept
- Prüfung der Wirksamkeit der Maßnahmen durch den Datenschutzbeauftragten in Zusammenarbeit mit der Geschäftsführung

6. Auftragskontrolle

- Verarbeitung nur entsprechend den dokumentierten Weisungen des Auftraggebers
- Weisungen erfolgen zwischen ausdrücklich bestimmten Vertragspersonen
- Eingesetzte Personen sind über datenschutzrechtliche Anforderungen informiert und schriftlich auf die Vertraulichkeit nach Art. 24, 29 und 32 Abs. 4 DSGVO verpflichtet
- Unterauftragnehmer werden sorgfältig im Hinblick auf die Eignung zur Einhaltung der maßgeblichen Sicherungsvorkehrungen geprüft und schriftlich zur Einhaltung der jeweils

anzuwendenden datenschutzrechtlichen Vorgaben verpflichtet

Anlage 2

Liste der Unterauftragnehmer



gemäß Art. 28 DSGVO

Name und Anschrift der weiteren Auftragnehmer	Beschreibung der Leistung
Ceos Solution GmbH Universitätsstr. 36a 44789 Bochum	Online Portal zur Eingabe von Abrechnungsdaten