Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

BFW LICHTENBERG
Messdienstleistungen und Heizkostenabrechnungen.

Aus Hamburg, für Ihre Immobilie. Für Sie im Einsatz.

zwischen
– Verantwortlicher, nachstehend **„Auftraggeber“** genannt –
und
BFW Lichtenberg Gesellschaft für Messdienstleistungen mbH, Lademannbogen 136, D-22339 Hamburg
– Auftragsverarbeiter, nachstehend **„Auftragnehmer“** genannt –

1. Gegenstand und Dauer der Verarbeitung
(1) Der Gegenstand dieser Vereinbarung zur Auftragsverarbeitung (nachfolgend „Vereinbarung“ genannt) und die Kontaktdaten des Auftraggebers ergeben sich aus dem jeweiligen Auftrag (nachfolgend „Auftrag“ genannt).

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

2. Konkretisierung des Inhalts der Verarbeitung
(1) Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in dem jeweiligen Auftrag konkret beschrieben. Die Verarbeitung durch den Auftragnehmer beinhaltet auch die Anonymisierung personenbezogener Daten und die Verarbeitung zu statistischen sowie wissenschaftlichen Zwecken, die für die zu erbringende Dienstleistung erforderlich sind.

Der Auftragnehmer verarbeitet Daten zweckgebunden und ausschließlich
im Rahmen der zwischen den Parteien getroffenen Vereinbarung und nach dokumentierter Weisung des Auftraggebers.

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.

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

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Mieter-/Wohnungseigentümerdaten (z. B. Name, Anschrift, Umlageschlüssel, Verbrauchsdaten)
- Auftragsdaten (z. B. Auftragsart, Status, Foto- und Videodokumentation)
- Mess- und Verbrauchswerte (insbesondere Stichtags- und Monatsendwerte)

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Mieter, Wohnungseigentümer

3. Technische und organisatorische Maßnahmen
(1) Der Auftragnehmer setzt die in Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen um. Die dokumentierten Maßnahmen sind Grundlage der Vereinbarung. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser abzustimmen und einvernehmlich und angemessen umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gemäß 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. 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 DS-GVO zu berücksichtigen.

(3) 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. Weisungsbefugnis des Auftraggebers
(1) Der Auftraggeber ist jederzeit zur Erteilung von Weisungen berechtigt. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach geändert, ergänzt oder ersetzt werden. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und können zusätzliche Kosten verursachen.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich erteilt. Mündlich erteilte Weisungen bestätigt der Auftraggeber mindestens in Textform.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung sei rechtswidrig. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Die Parteien benennen gegenseitig eine oder mehrere weisungsberechtigte und empfangsberechtigte Personen. Die Weisungen sind grundsätzlich an diese Person(en) zu richten.

5. Pflichten des Auftragnehmers
(1) Der Auftragnehmer setzt bei der Durchführung des Auftrags nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

(2) Der Auftragnehmer ist zur Umsetzung und Einhaltung aller für diese Vereinbarung erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (siehe Anlage 1) verpflichtet.

(3) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Kopien, soweit sie zur Erfüllung der Vereinbarung und zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DS-GVO, soweit sie sich auf diese Vereinbarung 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.

(5) 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 jeweils zu unterstützen.

(6) 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.

(7) Auf Anforderung stellt der Auftragnehmer dem Auftraggeber Informationen zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen zur Verfügung.

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 ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, wie Telekommunikationsleistungen, Post-, Transport-, Versanddienstleistungen, Reinigungsleistungen.

(2) Die vertraglich vereinbarten (Teil-)Leistungen werden unter Einbeziehung der in Anlage 2 genannten Unterauftragnehmer erbracht. Der Auftragnehmer darf weitere Unterauftragnehmer auf Grundlage der hier allgemein erteilten schriftlichen Einwilligung einsetzen. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung solcher Unterauftragnehmer mindestens 4 Wochen vor Beginn der Verarbeitung durch den Unterauftragnehmer, indem die jeweils aktuelle Liste der (beabsichtigten) Unterauftragnehmer unter der in Anlage 2 genannten Internetadresse zur Verfügung gestellt wird. Der Auftraggeber hat die Möglichkeit, sich jederzeit auf der o. g. Internetseite über den aktuellen Stand der (beabsichtigten) Unterauftragnehmer zu informieren, wodurch er die Möglichkeit erhält, gegen Änderungen Einspruch zu erheben. Wünscht der Auftraggeber eine aktive Benachrichtigung über beabsichtigte Unterauftragnehmer, teilt er dem Auftragnehmer seine E-Mail-Adresse an datenschutz@bfw-lichtenberg.de mit. Andernfalls verzichtet der Auftraggeber auf aktive Benachrichtigungen über beabsichtigte Unterauftragnehmer und informiert sich stattdessen regelmäßig auf der o. g. Internetseite.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/ des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nach Art. 44 ff. DS-GVO sicher.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der Genehmigung des Hauptauftragnehmers; sämtliche vom Auftragnehmer übernommenen Datenschutzpflichten aus dieser Vereinbarung sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich während der üblichen Geschäftszeiten von der Angemessenheit der beim Auftragnehmer getroffenen Maßnahmen zum Schutz der Daten in dessen Geschäftsbetrieb zu überzeugen. Vom Auftraggeber dafür eingesetzte Personen müssen sich gegenüber dem Auftragnehmer zur Geheimhaltung verpflichten. Die eingesetzten Personen dürfen in keiner Beziehung zu einem Wettbewerber des Auftragnehmers stehen. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Angemessenheit der beim Auftragnehmer getroffenen Maßnahmen zum Schutz der Daten 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) Der Nachweis geeigneter Maßnahmen kann auch erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revisionsstellen, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung im Rahmen von IT-Sicherheits- oder Datenschutzaudits (z. B. nach BSI-Grundschutz).

(4) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten informiert der Auftraggeber den Auftragnehmer unverzüglich.

8. Mitteilungs- und Unterstützungspflicht des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenschutzverletzungen, bei Datenschutz--Folgeabschätzungen und vorheriger 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 des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden; der Verlust eines Datenträgers, welcher keine besonderen Kategorien von Daten gemäß Art. 9 DS-GVO enthält und dessen gespeicherte personenbezogene Daten nach dem Stand der Technik verschlüsselt sind, sowie die Fehlversendung einer der Transportverschlüsselung unterliegenden elektronischen Nachricht (E-Mail) ohne besondere Kategorien von Daten gemäß Art. 9 DS-GVO an einen dem Auftragnehmer bekannten falschen Empfänger führen nach Einschätzung des Auftraggebers nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen und sind entsprechend vom Auftragnehmer zu dokumentieren und nicht in jedem Einzelfall weiterzuleiten. Der Auftragnehmer wird dem Auftraggeber die Dokumentation der Datenschutzverletzungen auf Anforderung vorzeigen
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen; insbesondere darf der Auftragnehmer die Daten, die im Rahmen dieser Vereinbarung verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers 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. Betreffend die Auskunftserteilung nach Art. 15 DS-GVO erteilt der Auftraggeber dem Auftragnehmer die Weisung, dem Betroffenen auf seinen Antrag hin, die in Bezug auf die durch den Auftragnehmer durchgeführte Datenverarbeitung notwendigen Auskünfte zu erteilen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9. Vergütung von datenschutzbezogenen Leistungen

(1) Der Auftragnehmer ist berechtigt, für Unterstützungsleistungen, die das notwendige Maß an Aufwand übersteigen, insbesondere nach Ziffern 6 und 8 dieser Vereinbarung, eine angemessene Vergütung nach Zeit- und Materialaufwand zu verlangen, sofern sie nicht in der Leistungsvereinbarung enthalten und nicht auf das Fehlverhalten des Auftragnehmers zurückzuführen sind sowie nicht ausschließlich in der Erfüllung der sich unmittelbar aus der DS-GVO bzw. dem BDSG ergebenden Pflichten des Auftragnehmers bestehen.

10. Löschung und Rückgabe von personenbezogenen Daten

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

BFW LICHTENBERG
Messdienstleistungen und Heizkostenabrechnungen.

Aus Hamburg, für Ihre Immobilie. Für Sie im Einsatz.

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

(2) Bezogen auf die Messwerte ist der Auftragnehmer angewiesen, die Monatsendwerte und die Stichtagswerte sechs Jahre nach Ende des Abrechnungszeitraums zu löschen.

(3) Von den Lösch- und Rückgabepflichten sind solche Daten ausgenommen, für die nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung besteht.

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

BFW LICHTENBERG
Messdienstleistungen und Heizkostenabrechnungen.

Aus Hamburg, für Ihre Immobilie. Für Sie im Einsatz.

Anlage 1 – technisch-organisatorische Maßnahmen

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

- Zutrittskontrollmaßnahmen
  - Zutrittsbeschränkungen für Unbefugte für nicht öffentliche Bereiche
  - Regelung zur Besucherkontrolle
  - Begleitung von Besuchern
  - Physikalischer Schutz, manuelles Schließsystem
  - Schlüsselregelung für alle Mitarbeiter
  - Server in separatem und abgeschlossenem Raum
  - Sorgfältige Auswahl von Reinigungspersonal
  - Hotline für IT-Notfälle
- Zugangskontrollmaßnahmen
  - Log-in nur mit individuellem Benutzernamen und Passwort
  - Definition von Rollen und Verantwortlichkeiten in einem Berechtigungskonzept
  - Passwortvergabe, sichere Passwörter
  - Einsatz von VPN-Technologie
  - Schutz vor Software mit Schadwirkung (Eset Software)
- Zugriffskontrollmaßnahmen
  - Berechtigungsvergabe erfolgt auf Basis eines definierten Prozesses
  - Reduzierte Anzahl an Administratoren
  - Auf PCs und Notebooks ist ein fortlaufend aktualisierter Virenschutz technisch sichergestellt
  - Passwortsicherheit durch Anforderungen an Länge, Komplexität und Wechsel von Passwörtern nach dem Stand der Technik
  - Einsatz von Aktenvernichtern
  - Verschlüsselung von Datenträgern
  - Sichere Vernichtung von Datenträgern

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

- Maßnahmen zur Weitergabekontrolle
  - Einrichtung von Standleitungen und VPN-Technologie
  - Sorgfältige Auswahl von Transportbehältern und Transportpersonal
  - Verbot der Datenweitergabe / Datenauswertung
  - Keine Weitergabe von Daten in anonymisierter Form
  - Verwendung exklusiver WAN-Verbindungen

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

- Maßnahmen zur Verfügbarkeitskontrolle
  - Unterbrechungsfreie Stromversorgung
  - Feuer- und Rauchmeldeanlage, Sprinkleranlage
  - Testen der Datenwiederherstellung
  - Erstellen eines Konzeptes für Backup und Recovery
  - Serverräume nicht unterhalb sanitärer Anlagen
  - Kontinuierliches Monitoring
  - Wartung und Sicherheitsupdates
- Maßnahmen zur Widerstandsfähigkeit- und Ausfallsicherheitskontrolle
  - Regelmäßige Wartung
  - Redundanz bei der Datenspeicherung
  - Regelmäßige Überprüfung der Rücksicherbarkeit von Datensicherungen

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

- Datenschutzmanagement
  - Datenschutzrichtlinie sowie definiertes Datenschutzmanagementsystem
  - Sensibilisierung und Schulung der Mitarbeiter zu Datenschutz und Datensicherheit
  - Mitarbeiter sind schriftlich auf die Vertraulichkeit verpflichtet
  - Implementierter Prozess zur Erfüllung von Betroffenenrechtsbegehren
  - Prozess zur Erforderlichkeitsprüfung und Durchführung von Datenschutzfolgenabschätzungen
- Auftragskontrolle
  - Vertragsstrafen bei Verstößen
  - Auswahl zuverlässiger Auftragnehmer

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

BFW LICHTENBERG
Messdienstleistungen und Heizkostenabrechnungen.

Aus Hamburg, für Ihre Immobilie. Für Sie im Einsatz.

Anlage 2 – Unterauftragnehmer

Firma	Anschrift	Leistungsgegenstand
BFW Büro für Wärmemesstechnik oHG	Am Sohlweg 32 76297 Stutensee	Rechenzentrum für Abrechnungsdienstleistungen
Objektus GmbH	Mollsfeld 3 40670 Meerbusch	Ablesung, Montage und Austausch von Rauchwarnmeldern
Michael Kruse	Volksdorfer Weg 191b 22393 Hamburg	Büro Dienstleistungen
ram electronic GmbH	Lütjenmoor 82 22850 Norderstedt	IT-Dienstleistungen und Consulting
ViSaDa Software Ferdinando Caballero	Feldweg 51 22844 Norderstedt	Software und Wartung
Verbund Messen und Abrechnen GmbH	Luxemburger Straße 1 45131 Essen	IT-Dienstleistungen, Abrechnungsdienstleistungen
finest-organizing Stina Klein	Dorfstr. 9a 24613 Aukrug	Büro Dienstleistungen
BFW Lichtenberg Servicepartner für Ablesung, Montage, Austausch	Listung auf Anforderung	Ablesung, Montage und Austausch