

## Auftragsverarbeitungsvertrag zwischen dem Auftraggeber (nachfolgend AG genannt) und der RMD GmbH als Auftragnehmer (nachfolgend AN genannt)

1. **Allgemeines**
- 1.1. Der AN verarbeitet personenbezogene Daten im Auftrag des AGs i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
- 1.2. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.
2. **Gegenstand des Auftrags**
- 2.1. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.
3. **Rechte und Pflichten des AGs**
- 3.1. Der AG ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den AN. Dem AN steht nach Ziff. 4 Abs. 5 das Recht zu, den AG darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
- 3.2. Der AG ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der AN wird den AG unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem AN geltend machen.
- 3.3. Der AG hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem AN zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
- 3.4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des AGs beim AN entstehen, bleiben unberührt.
- 3.5. Der AG kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in dem **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim AG ändern, wird der AG dies dem AN in Textform mitteilen.
- 3.6. Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den AN feststellt.
- 3.7. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den AG geltenden gesetzlichen Meldepflicht besteht, ist der AG für deren Einhaltung verantwortlich.
4. **Allgemeine Pflichten des ANs**
- 4.1. Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom AG erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den AN ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der AN dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des AGs. Eine hiervon abweichende Verarbeitung von Daten ist dem AN untersagt, es sei denn, dass der AG dieser schriftlich zugestimmt hat.
- 4.2. Der AN verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des AGs, die zumindest in Textform (z.B. E-Mail) erfolgen muss. Eine Zustimmung des AGs kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 –49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.
- 4.3. Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.
- 4.4. Der AN ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des AGs verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der AN wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem AG abstimmen.
- 4.5. Der AN wird den AG unverzüglich darüber informieren, wenn eine vom AG erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der AN ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den AG bestätigt oder geändert wird. Sofern der AN darlegen kann, dass eine Verarbeitung nach Weisung des AGs zu einer Haftung des ANs nach Art. 82 DSGVO führen kann, steht dem AN das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
- 4.6. Die Verarbeitung von Daten im Auftrag des AGs außerhalb von Betriebsstätten des ANs oder Subunternehmern ist nur mit Zustimmung des AGs in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den AG in Privatwohnungen ist nur mit Zustimmung des AGs in Schriftform oder Textform im Einzelfall zulässig.
- 4.7. Der AN wird die Daten, die er im Auftrag für den AG verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.
- 4.8. Der AN kann dem AG die Person(en) benennen, die zum Empfang von Weisungen des AGs berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in dem **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim AN ändern, wird der AN dies dem AG in Textform mitteilen.
5. **Datenschutzbeauftragter des ANs**
- 5.1. Der AN bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der AN trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Die Benennung des Datenschutzbeauftragten erfolgt in Anlage 4.
- 5.2. Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des AGs entfallen, wenn der AN nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der AN nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des AGs gewährleisten.
6. **Meldepflichten des ANs**
- 6.1. Der AN ist verpflichtet, dem AG jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des AGs, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der AN im Auftrag des AGs verarbeitet.
- 6.2. Ferner wird der AN den AG unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem AN tätig wird und dies auch eine Kontrolle der Verarbeitung, die der AN im Auftrag des AGs erbringt, betreffen kann.
- 6.3. Dem AN ist bekannt, dass für den AG eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der AN wird den AG bei der Umsetzung der Meldepflichten unterstützen. Der AN wird dem AG insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des AGs verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des ANs an den AG muss insbesondere folgende Informationen beinhalten:
  - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - eine Beschreibung der von dem AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls

Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

## 7. Mitwirkungspflichten des ANs

- 7.1. Der AN unterstützt den AG bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.
- 7.2. Der AN wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den AG mit. Er hat dem AG die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
- 7.3. Der AN unterstützt den AG unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

## 8. Kontrollbefugnisse

- 8.1. Der AG hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des AGs durch den AN jederzeit im erforderlichen Umfang zu kontrollieren.
- 8.2. Der AN ist dem AG gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.
- 8.3. Der AG kann eine Einsichtnahme in die vom AN für den AG verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.
- 8.4. Der AG kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des ANs zu den jeweils üblichen Geschäftszeiten vornehmen. Der AG wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des ANs durch die Kontrollen nicht unverhältnismäßig zu stören.
9. Der AN ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem AG i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den AG zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der AG ist über entsprechende geplante Maßnahmen vom AN zu informieren. **Unterauftragsverhältnisse / Unterauftragsnehmer (nachfolgend Unter-AN genannt)**
- 9.1. Die Beauftragung von Unter-ANn durch den AN ist nur mit Zustimmung des AGs in Textform zulässig. Der AN wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in dem **Anlage 3** zu diesem Vertrag angeben.
- 9.2. Der AN hat den Unter-AN sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen AG und AN getroffenen Vereinbarungen einhalten kann. Der AN hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unter-AN die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom AN zu dokumentieren und auf Anfrage dem AG zu übermitteln.
- 9.3. Der AN ist verpflichtet, sich vom Unter-AN bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unter-AN benannt worden ist, hat der AN den AG hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unter-AN gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.
- 9.4. Der AN hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des AGs auch gegenüber dem Unter-AN gelten.
- 9.5. Der AN hat mit dem Unter-AN einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der AN dem Unter-AN dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen AG und AN festgelegt sind. Dem AG ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
- 9.6. Der AN ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des AGs und von Aufsichtsbehörden auch gegenüber dem Unter-AN gelten und entsprechende Kontrollrechte von AG und Aufsichtsbehörden vereinbart werden.

Es ist zudem vertraglich zu regeln, dass der Unter-AN diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

- 9.7. Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der AN bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der AN für den AG erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der AN ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den AG genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des AGs verarbeitet werden.
10. **Vertraulichkeitsverpflichtung**
- 10.1. Der AN ist bei der Verarbeitung von Daten für den AG zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der AN verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem AG obliegen. Der AG ist verpflichtet, dem AN etwaige besondere Geheimnisschutzregeln mitzuteilen.
- 10.2. Der AN sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der AN sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat.
- 10.3. Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem AG auf Anfrage nachzuweisen.
11. **Wahrung von Betroffenenrechten**
- 11.1. Der AG ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der AN ist verpflichtet, den AG bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der AN hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den AG erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.
- 11.2. Soweit eine Mitwirkung des ANs für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den AG erforderlich ist, wird der AN die jeweils erforderlichen Maßnahmen nach Weisung des AGs treffen. Der AN wird den AG nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
- 11.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem AG beim AN entstehen, bleiben unberührt.
- 11.4. Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim AN geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der AG verantwortlich ist, ist der AN berechtigt, dem Betroffenen mitzuteilen, dass der AG der Verantwortliche für die Datenverarbeitung ist. Der AN darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.
12. **Vergütung**
- 12.1. Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.
13. **Technische und organisatorische Maßnahmen zur Datensicherheit**
- 13.1. Der AN verpflichtet sich gegenüber dem AG zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

- 13.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der AN im Voraus mit dem AG abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom AN ohne Abstimmung mit dem AG umgesetzt werden. Der AG kann jederzeit eine aktuelle Fassung der vom AN getroffenen technischen und organisatorischen Maßnahmen anfordern.
- 13.3. Der AN wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der AN den AG informieren.
- 14. Dauer des Auftrags**
- 14.1. Der Vertrag beginnt mit Unterzeichnung. Die Dauer dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung. Die Vereinbarung endet, ohne dass es einer Kündigung bedarf, mit Beendigung der Leistungsvereinbarung, nicht jedoch vor Erfüllung der Rückgabe- bzw. Löschpflichten.
- 14.2. Der AG kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des ANs gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der AN eine Weisung des AGs nicht ausführen kann oder will oder der AN den Zutritt des AGs oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

## Anlagen

### Anlage 1 - Gegenstand des Auftrags

- 1. Gegenstand und Zweck der Verarbeitung**
- 1.1. Der Auftrag des AGs an den AN umfasst folgende Arbeiten und/oder Leistungen:
- 1.2. Ausstattung zur Verbrauchserfassung**
- 1.2.1. Der AN installiert Verbrauchserfassungsgeräte, die selbständig Verbrauchsdaten für Heizwärme, Warmwasser und Kaltwasser erfassen. Die Verbrauchsdaten werden, soweit es sich um elektronische Geräte handelt, in den Verbrauchserfassungsgeräten gespeichert. Die Verbrauchswerte werden zum Zwecke der Weiterverarbeitung im Rahmen der Heiz- und Betriebskostenabrechnung manuell oder elektronisch ausgelesen und in die Datenverarbeitung des ANs übernommen. Soweit die Verbrauchserfassungsgeräte über eine Funkausstattung verfügen, werden die Verbrauchsdaten per Funk ausgelesen und an den AN pseudonymisiert übermittelt.
- 1.2.2. Die Ausstattung zur Verbrauchserfassung erfolgt nach der Maßgabe der gesetzlichen Verpflichtung aus der Heizkostenverordnung, der Landesbauordnung und den mietvertraglichen Verpflichtungen.
- 1.2.3. Adress- und Kommunikationsdaten werden für die Information und zur Abstimmung von Montageterminen verwendet.**
- 1.3. Ablesung und Abrechnung, uVI**
- 1.3.1. Die Verbrauchswerte werden zum Zwecke der Weiterverarbeitung im Rahmen der Heiz- und Betriebskostenabrechnung manuell oder elektronisch ausgelesen und in die Datenverarbeitung des ANs übernommen. Soweit die Verbrauchserfassungsgeräte über eine Funkausstattung verfügen, werden die Verbrauchsdaten per Funk ausgelesen und an den AN pseudonymisiert übermittelt.
- 1.3.2. Auf der Grundlage der Verbrauchswerte und unter Zugrundelegung der Wohnflächen und Nutzungszeiträume werden Verbrauchsabrechnungen nach der Heizkostenverordnung bzw. der mit den Nutzern vereinbarten Umlagevereinbarungen erstellt. Die Verbrauchserfassung und die verbrauchsabhängige Abrechnung erfolgt nach der Maßgabe der

### 15. Beendigung

- 15.1. Nach Beendigung des Vertrages hat der AN sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des AGs an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom AG gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem AG unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.
- 15.2. Der AN darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den AN eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.
- 16. Schlussbestimmungen**
- 16.1. Sollte das Eigentum des AGs beim AN durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der AN den AG unverzüglich zu informieren. Der AN wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
- 16.2. Für Nebenabreden ist die Schriftform erforderlich.
- 16.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

gesetzlichen Verpflichtung aus der Heizkostenverordnung, der Landesbauordnung und nach den mietrechtlichen Bestimmungen. Die Verbrauchswerte werden dem Bewohner monatlich gemäß HkVO zur Verfügung gestellt.

- 1.3.3. Adress- und Kommunikationsdaten werden für die Information und zur Abstimmung von Ableseterminen verwendet und bei der Erstellung der Abrechnungen angedruckt.
- 1.4. Weitere beauftragte Arbeiten und Leistungen  
Der AN erbringt bei Beauftragung folgende weitere Leistungen / Arbeiten:
- Legionellenprüfungen gemäß Trinkwasserverordnung
  - Erstellung von Energieausweisen
  - Montage- und Wartung/Inspektion von Rauchwarnmeldern
  - allgemeine Beratungsleistungen
- 2. Arten der personenbezogenen Daten**
- 2.1. Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:
- 2.2. Personenstammdaten, Adressdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Bankverbindungsdaten, Verbrauchsdaten von Wärme und Wasser der Mieter bzw. Bewohner, sonstige Energiedaten und Daten der Auswertung der Rauchwarnmelder- und Legionellenprüfungen.
- 3. Kategorien betroffener Person**
- 3.1. Kreis der von der Datenverarbeitung betroffenen Personen:
- 3.2. Mieter und Bewohner, Ansprechpartner Mietverwaltungen (Kunden), SUB-Unternehmer, technische Dienstleister, Mitarbeiter der RMD GmbH
- 4. Personen des ANs**
- 4.1. Weisungsberechtigte Personen des ANs sind der/die Geschäftsführer und der/die Prokuristen des ANs.
- 4.2. Es wurde ein externer Datenschutzbeauftragter schriftlich bestellt, der seine Tätigkeit gemäß Artikel 38 und 39 DSGVO ausübt.

**Anlage 2 - Technisch-organisatorische Maßnahmen – Bereich der RMD GmbH**

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

- Zutrittskontrolle  
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen möglich:
  - Pförtner
  - Alarmanlage mit Aufschaltung Wachschatz
  - Verschlussene Räume mit Datenverarbeitungsanlagen
  - Gäste werden innerhalb der Firmenräume begleitet
- Zugangskontrolle  
Keine unbefugte Systembenutzung:
  - sichere Kennwörter (min. 8 Zeichen sowie Komplexreglungen)
  - automatische Sperrmechanismen (3 Fehlversuche mit Zeitstaffelung)
- Zugriffskontrolle  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:
  - Berechtigungskonzept sowie bedarfsgerechte Zugriffsrechte
  - Protokollierung von Zugriffen
- Trennungskontrolle  
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:
  - Mandantenfähigkeit des IT - Systems,
  - Sandboxing (Datenaustausch)

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

- Weitergabekontrolle  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:
  - Virtual Private Networks (VPN), verschlüsselter Datenverkehr (mind. TLS 1.2)
- Eingabekontrolle
  - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben,

verändert oder entfernt worden sind:

- Protokollierung
- Dokumentenmanagementsystem

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

- Verfügbarkeitskontrolle
- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
  - mehrstufige Backup-Strategie (Arbeitsanweisung Backup)
  - unterbrechungsfreie Stromversorgung (USV)
  - mehrstufiges Virenschutzsystem, Firewall-System
  - Cluster des Netzwerkes
  - Klimatisierung
  - IT Notfallplan
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
  - regelmäßige Restoretests (Arbeitsanweisung Backup)

**4. 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  
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des AG:
  - Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement,
  - strenge Auswahl der Dienstleister,
  - Vorüberzeugungspflicht sowie Nachkontrollen

**Anlage 3 - Unterauftragnehmer (Unter-AN)**

Der AN nimmt für die Verarbeitung von Daten im Auftrag des AGs Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unter-AN“). Dabei handelt es sich um nachfolgende Unternehmen:

Lfd.Nr.	Firma	Adresse	Funktion der Leistungserbringung
1	KingTec - Computersysteme Riesa oHG	Am Anger 4, 01587 Riesa	Dienstleister im IT-Bereich
2	KUGU Home GmbH	Straßburger Straße 9 F , 10405 Berlin	Dienstleister im IT-Bereich
3	Dr. Reinhard Frekers	Teupenweg 5, 48496 Hopsten	Dienstleister im IT-Bereich
4	Eurofins Umwelt Ost GmbH	Löbstedter Straße 78, 07749 Jena	Dienstleister der Legionellenprüfung
5	Wolf Haustechnik	Leutewitzerstraße 59, 01589 Riesa	Dienstleister für Zählermontage, Prüfung und Ablesung
6	Epperlein GmbH	Rostocker Straße 50, 01587 Riesa	Dienstleister für Zählermontage, Prüfung und Ablesung
7	Volker König	Pausitzer Straße 2, 01589 Riesa	Dienstleister für Zählermontage, Prüfung und Ablesung

**Anlage 4 - Benennung des Datenschutzbeauftragten**

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Norbert Schütze, 03525/70351-0, datenschutz@brainmatrix.de bestellt. Ein Wechsel des Datenschutzbeauftragten wird auf der Internetseite des Auftragnehmers rmd-sachsen.de veröffentlicht.