**Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO**

zwischen

_____

_____

_____

_____

als Verantwortlicher (hier bezeichnet als *„Auftraggeber“*)

und

**Tenié und Gores GmbH**
**vertreten durch die Geschäftsführer**
**Stephan Kiermeyer und Eva Gürtzgen**
**Am Schornacker 23**
**46485 Wesel**

als Auftragsverarbeiter (hier bezeichnet als *„Auftragnehmer“*)

**Präambel**

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

**§ 1 Begriffsbestimmungen**

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

**§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde**

(1) Zuständige Aufsichtsbehörde für den **Auftraggeber** ist (**die zutreffende Behörde bitte ankreuzen!**):

| | | | |
|---|---|---|---|
| □ | Baden-Württemberg<br>Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg<br>Königstraße 10a<br>70173 Stuttgart<br>Telefon: 07 11/61 55 41-0<br>Telefax: 07 11/61 55 41-15 | □ | Bayern<br>Bayerisches Landesamt für Datenschutzaufsicht<br>Promenade 27 (Schloss)<br>91522 Ansbach<br>Telefon: 0981/53-1300<br>Telefax: 0981/53-5300<br>E-Mail: poststelle@lda.bayern.de |

| | | | |
|---|---|---|---|
| | E-Mail: poststelle@lfdi.bwl.de | | |
| ☐ | Berlin<br>Berliner Beauftragte für Datenschutz und Informationsfreiheit<br>Friedrichstraße 219<br>10969 Berlin<br>Telefon: 030/13 889-0<br>Telefax: 030/215-5050<br>E-Mail: mailbox@datenschutz-berlin.de | ☐ | Brandenburg<br>Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht<br>Stahnsdorfer Damm 77<br>14532 Kleinmachnow<br>Telefon: 03 32 03/356-0<br>Telefax: 03 32 03/356-49<br>E-Mail: poststelle@lda.brandenburg.de |
| ☐ | Bremen<br>Die Landesbeauftragte für Datenschutz und Informationsfreiheit<br>der Freien Hansestadt Bremen<br>Arndtstraße 1<br>27570 Bremerhaven<br>Telefon: 0421/361-2010<br>Telefax: 0421/496-18495<br>E-Mail: office@datenschutz.bremen.de | ☐ | Hamburg<br>Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit<br>Klosterwall 6 (Block C)<br>20095 Hamburg<br>Telefon: 040/42854-4040<br>Telefax: 040/42854-4000<br>E-Mail: mailbox@datenschutz.hamburg.de |
| ☐ | Hessen<br>Der Hessische Datenschutzbeauftragte<br>Gustav-Stresemann-Ring 1<br>65189 Wiesbaden<br>Telefon: 06 11/140 80<br>Telefax: 06 11/14 08-900<br>E-Mail: poststelle@datenschutz.hessen.de | ☐ | Mecklenburg-Vorpommern<br>Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern<br>Lennéstraße 1, Schloss Schwerin<br>19053 Schwerin<br>Telefon: 0385/59494-0<br>Telefax: 0385/59494-58<br>E-Mail: info@datenschutz-mv.de |
| ☐ | Niedersachsen<br>Die Landesbeauftragte für den Datenschutz Niedersachsen<br>Prinzenstr. 5<br>30159 Hannover<br>Telefon: 05 11/120-45 00<br>Telefax: 05 11/120-45 99<br>E-Mail: poststelle@lfd.niedersachsen.de | **X** | Nordrhein-Westfalen<br>Landesbeauftragte für Datenschutz und Informationsfreiheit<br>Nordrhein-Westfalen<br>Kavalleriestraße 2-4<br>40213 Düsseldorf<br>Telefon: 0211/38424-0<br>Telefax: 0211/38424-10<br>E-Mail: poststelle@ldi.nrw.de |
| ☐ | Rheinland-Pfalz<br>Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz<br>Hintere Bleiche 34<br>55116 Mainz<br>Telefon: 061 31/208-24 49<br>Telefax: 061 31/208-24 97<br>E-Mail: poststelle@datenschutz.rlp.de | ☐ | Saarland<br>Unabhängiges Datenschutzzentrum Saarland<br>Fritz-Dobisch-Straße 12<br>66111 Saarbrücken<br>Telefon: 06 81/947 81-0<br>Telefax: 06 81/947 81-29<br>E-Mail: poststelle@datenschutz.saarland.de |
| ☐ | Sachsen<br>Der Sächsische Datenschutzbeauftragte<br>Devrientstraße 1<br>01067 Dresden<br>Telefon: 03 51/49 3-5401<br>Telefax: 03 51/49 3-5490<br>E-Mail: saechsdsb@slt.sachsen.de | ☐ | Sachsen-Anhalt<br>Landesbeauftragter für den Datenschutz Sachsen-Anhalt<br>Leiterstraße 9<br>39104 Magdeburg<br>Telefon: 03 91/818 03-0<br>Telefax: 03 91/818 03-33<br>E-Mail: poststelle@lfd.sachsen-anhalt.de |
| ☐ | Schleswig-Holstein<br>Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein<br>Holstenstraße 98<br>24103 Kiel<br>Telefon: 0431/988-1200<br>Telefax: 0431/988-1223<br>E-Mail: mail@datenschutzzentrum.de | ☐ | Thüringen<br>Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit<br>Häßlerstraße 8<br>99096 Erfurt<br>Telefon: 03 61/57 311 29 00<br>Telefax: 03 61/57 311 2904<br>E-Mail: poststelle@datenschutz.thueringen.de |

(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Nordrhein-Westfalen ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Kavalleriestraße 2-4, 40213 Düsseldorf
Telefon: 0211/38424-0 Telefax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

## § 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Heiz- und Nebenkostenabrechnungen für im Eigentum oder in Verwaltung des Auftraggebers stehende Immobilien auf Grundlage des folgenden Vertrages bzw. folgender Verträge:

***- Aktenzeichen:*** _____
***- Aktenzeichen:*** _____

-Alternativ fügen Sie bitte eine Anlage mit der Auflistung Ihrer Liegenschaften bei-

(nachfolgend *„Hauptvertrag“*). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

## § 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus **Anlage 5**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

## § 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 2** dargestellt. 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.

## § 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 3** aufgeführten Maßnahmen der

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer nach eigenem Ermessen vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als externer, betrieblicher Datenschutzbeauftragte bestellt: Herr Alexander Bugl, Bugl & Kollegen GmbH, Eifelstraße 55, 93057 Regensburg. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

## § 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichen“ im Sinne der DS-GVO liegt.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

### § 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

### § 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 4** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

### § 10 Anfragen und Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

### § 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

## § 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

## § 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

## § 14 Inkrafttreten, Schlussbestimmungen

(1) Dieser Vertrag wird ab dem 25. Mai 2018 wirksam und ersetzt mit ihrem Wirksamwerden ggf. bestehende frühere Auftragsverarbeitungsverträge, die die Parteien für die vertragsgegenständliche Datenverarbeitung zur Abwicklung des Hauptvertrages geschlossen haben.

(2) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(5) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Duisburg.

**Anlagen**
Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien
Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen
Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers
Anlage 4 – Genehmigte Subunternehmer
Anlage 5 – Weisungsberechtigte Personen

| | |
|---|---|
| Ort, Datum …….. | Wesel, den …….. |
| ……... | ……... |
| Für den Auftraggeber | Für die Tenié und Gores GmbH |

**Anlage 1 – Beschreibung der Art der verarbeiteten Daten/Datenkategorien**

Daten der betroffenen Personen:

- Vorname
- Nachname
- Anschrift (Straße, Hausnummer, Wohnort und Postleitzahl)
- Wohnungsgröße des Betroffenen
- Einzugs- und Auszugsdatum des Betroffenen
- Ggf. Personenanzahl im Haushalt des Betroffenen
- Ggf. Wohnungsnummer/Nummer der Wohneinheit des Betroffenen
- Ggf. Telefonnummer des Betroffenen.

**********

**Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen**

Die personenbezogenen Daten folgender Betroffener sind Gegenstand der Auftragsverarbeitung:

- Mieter (Kunden) des Auftraggebers
- Geschäftspartner des Auftraggebers

**********

**Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers**

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen Folgendes ein:

***Gewährleistung der Vertraulichkeit***

**Zutrittskontrolle**

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Schlüsselregelung mit einer Liste
- Serverräume sind abgegrenzt (Sperrbereich), kein Zugang für Unbefugte
- Anwesenheitskontrolle durch Zeiterfassungssystem und Schichtbuch (Produktion)
- Besucher nur in Begleitung durch Mitarbeiter
- Empfang ohne Rezeption
- Gebäude ist ein reines Bürogebäude
- Klingelanlage ohne Kamera
- Kontrolle der Reinigungs-und Wartungsarbeiten
- Mechanische Türschlösser
- Sorgfalt bei der Auswahl des Reinigungspersonals
- Trennung von Bearbeitungs- und Publikumszonen

**Zugangskontrolle**

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Maßnahmen:

- Login mit Benutzername und Passwort
- Es erfolgt eine Protokollierung der Benutzeranmeldungen und der jeweiligen Zeitpunkte
- Regelmäßiges Update der Firewall laufend und manuell
- Firewall
- Erstellen von Benutzerprofilen
- Anti-Virus-Clients
- Automatische Desktopsperre
- Bildschirmsperre mit Passwortaktivierung
- Lösch-/Sperrkonzept
- Passwortvergabe durch einen Administrator
- Zuordnung von Benutzerrechten
- Verwalten von Benutzerberechtigungen

**Zugriffskontrolle**

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, kopiert, verändert oder entfernt werden können.

Maßnahmen:

- Abschließbare Schränke für Sicherungsdatenträgern
- Aktenschredder (mind. Stufe 3 – cross cut)
- Protokollierung von Datenänderungen
- Protokollierung der Berechtigungen
- Protokollierung von Zugriffen auf Anwendungen (bei einer Änderung von Daten)
- Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger
- Autorisierungsprozess für Berechtigungen
- Vier-Augen-Prinzip
- Profile / Rollen
- Bildschirmsperre über Funktionstasten möglich
- Differenzierte Berechtigungen (Daten)
- Einsatz Rechte-/Rollenkonzept
- Das Siegel-User-Passwort-Prinzip ist umgesetzt. Für Passworte existiert eine Vorgabe zur Komplexität. Die Gültigkeit der Passwörter ist auf Tage begrenzt. Eine Rechteverwaltung ist implementierter.
  Die Fähigkeit der Systeme ist durch Auslegung, Update und Betreuung sichergestellt.
  Die Vertraulichkeit von Verbindungen ist durch entsprechende Verschlüsselungen sichergestellt.
- Schutz der IT-Infrastruktur durch Firewalls

**Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen
- Trennung von Arbeitsplätzen und Server

***Gewährleistung der Integrität***

**Weitergabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

- Verschlüsselter Mailanhang
- Email-Verschlüsselung
- Gesicherter Filetransfer
- Gesicherter Datentransfer
- Fernwartung für Hardware, Software, Anwendungen mit Protokollierung, Protokollauswertung
- Regelungen zum Umgang mit mobilen Speichermedien
- Verschlüsselung/Nutzung von VPN-Tunneln bei Übertragungen

**Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Vergabe von Rechten zur Bearbeitung von Daten

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Rechte- und Rollenkonzepts
- Berechtigungskonzept

***Pseudonymisierung und Verschlüsselung***

**Pseudonymisierung**

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Verwendung von Kundennummern

**Verschlüsselung**

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Verschlüsselung des Transports von E-Mails

***Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit***

**Verfügbarkeit (der Daten)**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Backup & Recovery-Konzept
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Unterbrechungsfreie Stromversorgung (USV)
- Datensicherungskonzept vorhanden
- Kontrolle des Sicherungsvorgangs
- RAID System / Festplattenspiegelung
- Datenarchivierung mit Archivierungskonzept

**Belastbarkeit (der Systeme)**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Einspielen von Sicherheitsupdates auf allen Entwicklersystemen
- Spamfilter
- Einsatz von Software Firewalls
- Notfallplan
- Die Belastbarkeit ist durch Auslegung und Überwachung der Systeme sichergestellt.

**Wiederherstellbarkeit (der Daten / der Systeme)**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Serverraum ist klimatisiert
- Brandschutztüren
- Feuerlöscher im Serverraum

- Feuerfeste Schränke
- Rauchverbot in Server- und PC-Arbeitsräumen
- Serverraum hat keine Fenster
- Serverraum ist getrennt von Arbeitsplätzen
- Serverräume oberhalb der Wassergrenze
- Schutzsteckdosenleisten im Serverraum
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums

***Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit***

**Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Verpflichtung der Mitarbeiter des Auftragnehmers auf das spezielle Geheimhaltungsvorschriften
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten (bei Bestellpflicht)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO)
- Abschluss eines Basisvertrags / einer Kundenvereinbarung (soweit personenbezogene Daten verarbeitet werden zusätzlich Abschluss eines Auftragsverarbeitungsvertrag)
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Eingesetzte Personen sind über datenschutzrechtliche Anforderungen informiert und schriftlich auf die Vertraulichkeit nach Artt. 24, 29 und 32 Abs. 4 DS-GVO verpflichtet
- Formalisierte Auftragserteilung
- Kriterien zur Auswahl der Auftragnehmer festgelegt (Referenzen, Zertifizierungen / Gütesiegel, Vorlage Datensicherheitskonzeption, Preis & Folgekosten, Lieferzeiten
- Regelung / Wahrung von Betroffenenrechten
- Regelung zum Einsatz von Subunternehmern
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags
- Unterauftragnehmer werden sorgfältig im Hinblick auf die Eignung zur Einhaltung der maßgeblichen Sicherungsvorkehrungen geprüft und schriftlich zur Einhaltung der jeweils anzuwendenden datenschutzrechtlichen Vorgaben verpflichtet

**Datenschutz-Management**

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Datenschutz-/Datensicherheitskonzept
- Datenschutzrichtlinie
- Bestellung eines externen Datenschutzbeauftragten
- Benennung eines internen Datenschutzkooridnators
- Verpflichtung der Mitarbeiter auf Vertraulichkeit
- Schulung der Mitarbeiter zum Datenschutz
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz

- Durchführung von Datenschutzfolgeabschätzungen (bei Bedarf)
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO
- Prozess zum Umgang mit Datenschutzverletzungen
- Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt)

**Incident-Response-Management**

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle
- Einsatz von Firewall und deren regelmäßige Aktualisierung
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung
- Notfallkonzept
- Vier-Augen-Prinzip bei wichtigen Datenverarbeitungen

**Datenschutzfreundliche Voreinstellungen**

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind (Datenminimierung Art. 5 Abs. 1 lit. c) DSGVO)
- Gewährleistung einer einfachen Ausübung des Widerrufsrechts eines Betroffenen

**Anlage 4 – Genehmigte Subunternehmer**

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

- addv.net, Inhaber Arno Duwe (Einzelfirma), Am Weißen Stein 31, 46487 Wesel-Büderich
- Allmess GmbH, GF Harald Jöllenbeck, Johannes Huizing, Chantel Landers, Joel Vach, Am Vossberg 11, 23758 Oldenburg
- CEOS Solution GmbH, GF Pantelis Radouniklis, Universitätsstraße 36 A, 44789 Bochum
- Computer Burkhard Overmann, Inhaber Burkhard Overmann, Hertener Straße 84, 45659 Recklinghausen
- E.G.O. domus GbR, Inhaber Jörg Freidank, Summter Chaussee 17,

  16515 Oranienburg
- Engelmann Sensor GmbH, GF Michael Keuthen, Dietrich Fabricius, Rudolf-Diesel-Straße 24-28, 69169 Wiesloch
- Ifena GmbH, GF Stephan Kiermeyer, Norisstraße 10, 91257 Pegnitz
- Gerstenberg GbR, Inhaber Andreas Gerstenberg, Am Mühlenberg 6, 40549 Düsseldorf
- Konietzko GmbH, Inhaber Gerald Konietzko, Fallgatter 6, 44369 Dortmund
- Officium GmbH, GF Stephan Kiermeyer, Jan-Christoph Wiemann, Norisstraße 10, 91257 Pegnitz
- Qundis GmbH, GF Volker Eck, Jörg Hattenbach, Sonnentor 2, 99098 Erfurt
- Tenié u. Gores GmbH SZB, GF Stephan Kiermeyer, Gewerbepark 16, 08340 Schwarzenberg
- Thermorent Messpartner GmbH, vertreten durch Geschäftsführer Frank Göbl, Michael Göbl, Richtweg 87, 90530 Wendelstein
- Ei Electronics GmbH, vertreten durch Vertretungsberechtigte: Philip Kennedy, Tobias Küpper, Franz-Rennefeld-Weg 5, 40472 Düsseldorf
- HMS Hanse Montageservice GmbH, GF Tino Säuberlich, Neu Roggentiner Straße 34 A, 18184 Roggentin

**********

**Anlage 5 – Weisungsberechtigte Personen**

**Weisungsberechtigte Personen des Auftraggebers sind**

Name, Vorname: ……
Adresse: ……
Telefon-Nummer: ……
Fax-Nummer: ……
Emailadresse: ……

Name, Vorname: ……
Adresse: ……
Telefon-Nummer: ……
Fax-Nummer: ……
Emailadresse: ……

**Weisungsempfänger beim Auftragnehmer sind**

Name, Vorname: Eva Gürtzgen
Adresse: Tenié und Gores GmbH, Am Schornacker 23, 46485 Wesel
Telefon-Nummer: 0281 – 206 21 18
Emailadresse: Eva.Guertzgen@tenieundgores.de

Name, Vorname: Walenciak, Kerstin
Adresse: Tenié und Gores GmbH, Am Schornacker 23, 46485 Wesel
Telefon-Nummer: 0281 – 206 21 -0
Emailadresse: Kerstin.Walenciak@tenieundgores.de

Name, Vorname:
Adresse:
Telefon-Nummer:
Emailadresse:

Name, Vorname:
Adresse:
Telefon-Nummer:
Emailadresse:

Name, Vorname:
Adresse:
Telefon-Nummer:
Emailadresse:

**********