Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (AV-Vertrag)

Zwischen

Immofolia Accounting GmbH

Willy-Brand-Straße 23, 20457 Hamburg

- im Folgenden „Auftragnehmer“ genannt -

und

Auftraggeber gemäß Angebot

- im Folgenden „Auftraggeber“ genannt –

- die Vorstehenden im Folgenden auch gemeinsam „Parteien“ genannt -

wird folgender Dienstleistungsvertrag geschlossen:

Präambel

Auftraggeber und Auftragnehmer sehen sich den hohen Standards verpflichtet, die durch die Datenschutzgrundverordnung und andere datenschutzrechtlichen Vorschriften gelten.

Zur Sicherung der Vertraulichkeit und Wahrung aller einschlägigen datenschutzrechtlicher Bestimmungen schließen die Parteien nachfolgende Vereinbarungen, die Anwendung auf alle Tätigkeiten finden, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Der vorliegende Auftragsverarbeitungsvertrag (kurz: „AVV“) konkretisiert für alle Verarbeitungen die Rechte und Pflichten der Parteien auf dem Gebiet des Datenschutzes, welche sich aus den zwischen den Parteien bereits oder künftig bestehenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen (kurz: „Hauptvertrag“) ergeben.

Der AVV kommt mit all seinen Teilen zur Anwendung, sofern und soweit der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (kurz: „Daten“) verpflichtet hat. Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten« im Sinne des Art. 4 Nr. 1 DSGVO) des Auftraggebers verarbeiten.

Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV und all seiner Teile den Regelungen des zugehörigen Hauptvertrages vor.

Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „Spezifika“) werden vor Beginn der Verarbeitung geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen, die Übersicht über Subauftragsnehmer sowie die technischen und organisatorischen Maßnahmen (kurz: „TOMs“).

§1 Gegenstand des Vertrages

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages als Anlage zum Hauptvertrag. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§2 Umfang der Verarbeitung

Die Dauer des Auftrages sowie Art und Zweck der Verarbeitung ergeben sich aus dem schriftlichen Hauptvertrag. Dieser AVV konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Hauptvertrag und der Auftragsverarbeitung ergeben. Er findet Anwendung auf alle in ihren Einzelheiten beschriebenen Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen.

Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich in dem Umfang, der zur Erfüllung der vereinbarten Leistungen gemäß Angebot erforderlich ist.

§3 Dauer

Die Auftragsverarbeitung beginnt mit der Annahme des Angebots des Auftragnehmers durch den Auftraggeber und endet mit der Kündigung des allgemeinen Dienstleistungsvertrages durch den Auftraggeber oder Auftragnehmer unter Einhaltung der Kündigungsfrist gemäß des allgemeinen Dienstleistungsvertrages.

§4 Kategorien der betroffenen Personen

Folgende Kategorien von Betroffenen sind Gegenstand des Auftrags:

- Kunden und Kunden des Auftraggebers sowie Mitarbeiter
- Mitarbeiter des Auftraggebers
- Informationen zum Auftraggeber selbst sowie Ansprechpartner
- Auftragsverarbeiter
- Lieferanten
- Personen, die über Kontobewegungen des Kunden identifizierbar sind

§5 Art der bezogenen Daten

Der Auftraggeber stellt dem Auftragnehmer sämtliche zur Auftragserfüllung notwendigen personenbezogenen Daten zur Verarbeitung zur Verfügung.

Folgende Datenarten sind Gegenstand dieser Auftragsverarbeitung:

§5.1. Allgemein

- Daten von Kunden (Eigentümern, Wohneigentümergemeinschaften, Vermietern, Mietern und ggf. Mietinteressenten) des Kunden, insbesondere Identifiktationsdaten, Kommunikation und Schriftverkehr, Kundenverträge und Vertragsdaten, Abrechnungen, Zahlungsinformationen, Bonitätsauskünfte;
- Daten über Zahlungs- und Kontobewegungen des Kunden und der Kunden des Kunden (bei Nutzung des entsprechenden Services), insbesondere Zahlungsempfänger/-absender, Verwendungszweck, Kontodaten, Beträge;
- Daten über Mitarbeiter, Beauftragte und Geschäftspartner des Kunden (z.B. Namen, E-Mail-Adressen, ggf. Benutzernamen bei der Anlage von Mitarbeiter-Accounts). Soweit sich Geschäftspartner des Kunden selbst bei Impower registrieren (z.B. Hausmeister) oder deren Daten nicht vom Auftraggebers zur Verfügung gestellt werden, werden diese Daten jedoch nicht im Auftrag des Auftraggebers verarbeitet.
- „Personenbezogene Daten“ oder „Daten“ im Sinne dieser Vereinbarung sind nur solche personenbezogenen Daten, die Impower im Auftrag des Kunden verarbeitet.

§.5.2. Spezifisch

- Identifikationsdaten
  - Vor- und Nachname/Titel
  - Geburtsdatum/Geburtsort
  - Straße/Hausnummer
  - Wohnort/Postleitzahl
  - Land
  - Telefon/Mobiltelefon/Fax
  - E-Mail-Adresse
  - Rolle
  - Anrede
- Abrechnungsdaten / Vertragsdaten
  - Bank/Kreditkarten-Informationen
  - Rechnungsdaten
  - Mahndaten (Mahngrund)
  - Korrespondenz/Schriftverkehr
- Individuelle Daten
  - - Termindaten
  - - Nationalität/Sprache
  - - Familienstand
  - - Fotos
- Mitarbeiterdaten
  - Mitarbeiterorganisationsinformationen (Telefon, Mobil, Fax, E-Mail)
  - Mitarbeiterstandortinformationen (Hausnummer, Straße, Stadt, PLZ)
  - Interne Sicherheitsdaten (Gruppen ID, Zertifikate, Zugriffsrechte)
  - Abteilung/Rolle

- Kommunikationsdaten /Systemdaten
    - Login / Passwörter
    - Protokolldaten (Log-in/Log-off)
    - Systemdaten (Konfigurationsinformationen, Alarmmeldungen)

§6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung ein-gesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftrag-nehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

§7 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

(4) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

§8 Sicherheit der Verarbeitung

(1) Die im **Anhang 1** beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jeder-zeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftrag-nehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier verein-barten Datenschutzniveaus ausgeschlossen ist.

(6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit an-gemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(7) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Auftraggeber jederzeit auf Verlangen vorzulegen.

§9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. 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;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen An-laufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ansprechpartner in datenschutzrechtlichen Angelegenheiten des Auftragnehmers ist: Alexander Stade

Beim Auftragnehmer besteht auskunftsgemäß zum Zeitpunkt des Vertragsabschlusses keine Bestellpflicht für einen Datenschutzbeauftragten nach Art. 37 DSGVO und §38 BDSG. Für die Einhaltung der gesetzlichen Bestellpflicht haftet der Auftragnehmer. Änderungen in der Bestellpflicht sind dem Auftraggeber unverzüglich mitzuteilen.

Ansprechpartner in datenschutzrechtlichen Angelegenheiten beim Auftraggeber ist der jeweils bestellte Datenschutzbeauftragte.

Ergeben sich bei den Ansprechpartnern und Datenschutzbeauftragten Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

(3) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(5) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

§ 10 Unterbeauftragung weiterer Auftragsverarbeiter

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten, die Gegenstand dieser Auftragsverarbeitung sind, ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „Unterauftragnehmer“) erbringen lassen Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

(2) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

(3) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(4) Die Verpflichtung des Unterauftragnehmer muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(6) Eine Beauftragung von Unterauftragnehmer in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln) erfüllt sind. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber

Subunternehmern gelten. In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmer deutlich voneinander abgegrenzt werden

(7) Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt Dazu zählen z.B. Post, Telekommunikationsleistungen, reine technische Wartung, Reinigungskräfte, Prüfer.

(8) ☒ Für die Durchführung der vereinbarten Auftragsverarbeitung durch Auftragnehmer sind Unterauftragsnehmer im Sinne des Art. 28 (4) tätig, siehe **Anhang 2**.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheits-beschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden.

§11 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen bei Abschluss des Vertrages.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

§12 Beendigung des Vertrages

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach Beendigung des Vertrages zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Rest-informationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

§13 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

§14 Haftung

(1) Der Auftragnehmer haftet für Schäden, die dem Auftraggeber durch die Verletzung seiner Pflichten aus diesem Vertrag entstehen, nur dann, wenn er diese Pflichtverletzung vorsätzlich oder grob fahrlässig begangen hat.

(2) Der Auftragsverarbeiter haftet nicht für Schäden, die dem Auftraggeber durch die Verarbeitung der personenbezogenen Daten entstehen, soweit diese Schäden nicht auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragsverarbeiters beruhen.

§15 Schlussbestimmungen

(1) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

(2) Sollten einzelne Teile dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. Anstelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.

(3) Es gilt die DSGVO und deutsches Recht.

Anhang 1 - TOMs des Auftragsverarbeiters

Es werden folgende auftragsspezifische technische und organisatorische Maßnahmen (TOMs) für den Auftragsverarbeiter vereinbart:

1.1 Zutrittskontrolle

Sonstige Maßnahmen: M365 mit GEO Einstellung Deutschland

1.2 Zugangskontrolle

Login mit Benutzername + Passwort
Automatische Sperrung von Nutzer-Accounts nach mehrfacher Fehleingabe von Passwörtern
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität
Zwei-Faktor-Authentifizierung
BIOS-Passwörter
Mobile Device Management-System
Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern
Prozess zum Rechteentzug bei Austritt von Mitarbeitern
Kontrollierte Vernichtung von Datenträgern
Verschlüsselung von mobilen Datenträgern
Anti-Viren-Software
Automatische Sperrmechanismen bei Mobil-Geräten
Firewall
Einsatz von Intrusion-Detection-Systemen

1.3 Zugriffskontrolle

Anzahl der Administratoren auf das „Notwendigste“ reduziert
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
Konzept der Laufwerksnutzung und -Zuordnung
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
Regelmäßige Überprüfung der Berechtigungen
Netzsegmentierung
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
Protokollieren von Dateizugriffen
Anti-Viren-Software
Schadsoftware-Filterung für Web
Schadsoftware-/Spam-Filterung für E-Mail
Firewall
Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger, z.B. Kopierschutz, Sperrung von USB-Ports, Data Loss Prevention (DLP)
Security Information & Event Management (SIEM)
Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)

1.4 Trennungskontrolle

Verarbeitung auf getrennten Systemen
Berechtigungskonzept
Laufwerkstrennung, verschiedene logische Laufwerke
Trennung von Entwicklungs-, Test- und Produktivsystem

2 Pseudonymisierung

manuelle Vergabe von Alias

3 Integrität

(Art. 32 Abs. 1 b DSGVO)

3.1 Weitergabekontrolle

Berechtigungskonzept
Protokollierung von Datenübertragung oder Datentransport
Protokollierung der Zugriffe und Abrufe
Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
Fernwartungskonzept (Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort etc.)
Verwaltung von Datenträgern, Bestandskontrolle
Dokumentation der Übermittlungsstellen und -wege
Verpackungs- und Versand Vorschriften
Direktabholung, Kurierdienst, Transportbegleitung
Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
Vollständigkeits- und Richtigkeitsprüfung
Firewall

3.2 Eingabekontrolle

Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Sicherheits-/Protokollierungssoftware
Systemseitige Protokollierung von Dateneingaben / -löschungen

3.3 Verschlüsselung

Verschlüsselung von Laptops
Verschlüsselte Aufbewahrung von Passwörtern
Verschlüsselter E-Mail-Versand (Transportverschlüsselung)
E-Mailversand verschlüsselter /passwortgeschützter Dateien
Verschlüsselung von Online-Diensten (HTTPS)
Sicherer Dateiaustausch (SFTP/FTPS)
Verschlüsselung bei Speicherung in Clouds und anderen externen Storage-Lösungen
Verschlüsselung bei Übertragung über Netzwerke (leitungsgebunden)
Verschlüsselung bei Übertragung über Funk-Netzwerke (WLAN)

4 Verfügbarkeit und Belastbarkeit

Server in separatem Brandabschnitt
Klimatisierte Serverräumlichkeiten
Blitz-/Überspannungsschutz
Unterbrechungsfreie Stromversorgung (USV)
RAID-Systeme
Systemhärtung (Abschaltung nicht benötigter Komponenten)
Automatische Updates Software und Firmware
Getrennte Partitionen für Betriebssysteme und Daten
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
Datensicherungs- und Backupkonzept
Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitten
Virenschutz
Firewall
Regelmäßige Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Netze und IT-Systeme)

Anhang 2 - Genehmigte Unterauftragnehmer

Folgende Unterauftragnehmer sind für die Erbringung von Teilleistungen im Rahmen dieses Auftragsverarbeitungsvertrages für uns tätig und gelten als genehmigt:

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Messdienstleister sowie Verwaltungssoftware und/oder Portalsoftware	Gem. Kundenvorgaben	Erstellen von Heizkostenabrechnungen, Verwalten von Wohn- oder Gewerbeeinheiten sowie die Kommunikation mit dem Endkunden
Impower GmbH	Sandstr. 33, 80335 München	Verwaltungssystem
HubSpot, Inc.	Gem. dem jeweils gültigen Nachträgen zum Datenschutz für Hubspot-Produkte und -Services	Verwaltungssystem
Verwaltungssysteme generell	Gem. Kundenvorgaben	Verwaltungssystem
Microsoft	Gem. dem jeweils gültigen Nachträgen zum Datenschutz für Microsoft-Produkte und -Services	Software-Dienst
Google (LLC und Untergesellschaften)	Gem. dem jeweils gültigen Nachträgen zum Datenschutz für Google-Produkte und -Services	Software-Dienst
EstateFlow GmbH	Willy-Brandt-Str. 23, 20457 Hamburg	Software-Dienst