Vereinbarung zur Auftragsverarbeitung

(gemäß Art. 28 DSGVO)

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [*Datum*]

- nachfolgend „Leistungsvereinbarung“ -

zwischen der
Bundesanstalt für Immobilienaufgaben (BImA), Ellerstraße 56, 53119 Bonn

vertreten durch

XXXXXX XXXX
- nachfolgend „Verantwortliche“ -

und

[*Vertragspartner/in*]
- nachfolgend „Auftragsverarbeiterin bzw. Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung *(*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - *DSGVO),* und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung der Verantwortlichen verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Beschäftigten der Auftragsverarbeiterin bzw. des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter betreffen.

(2) Dieser Vertrag gilt vorranging vor anderen Vereinbarungen und Abreden zwischen Verantwortlicher und Auftragnehmerin bzw. Auftragnehmer, es sei denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung, die dieser Vereinbarung angefügt ist.

(2) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter:

[Datenarten & -kategorien einfügen, bspw. Personenstammdaten, Kontaktdaten, bestimmte Gesundheitsdaten oder Verweis auf Leistungsbeschreibung im Anhang]

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen umfasst (Kategorien betroffener Personen):

[Aufzählung und Beschreibung der betroffenen Personenkreise, bspw. Beschäftigte, BewerberInnen, Veranstaltungsteilnehmende oder Verweis auf Leistungsbeschreibung im Anhang]

(4) Im Rahmen der Auftragsverarbeitung werden *[keine]* besondere*[n]* Kategorien von Daten verarbeitet.

(5) Die verarbeiteten personenbezogenen Daten haben einen *[normalen/ hohen]* Schutzbedarf.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die ihnen durch die Datenschutzgesetze (insb. DSGVO) auferlegten Pflichten einzuhalten. Die Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt die Auftragsverarbeiterin bzw. der Auftragsverarbeiter die Verantwortliche angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an die Auftragsverarbeiterin bzw. den Auftragsverarbeiter wendet, wird die Auftragsverarbeiterin bzw. der Auftragsverarbeiter dieses Ersuchen unverzüglich an die Verantwortliche weiterleiten.

(4) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen der Verantwortlichen verarbeiten, sofern sie bzw. er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem die Auftragsverarbeiterin bzw. der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt die Auftragsverarbeiterin bzw. der Auftragsverarbeiter der Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang der Auftragsverarbeiterin bzw. des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter hat die Verantwortliche unverzüglich zu informieren, wenn sie bzw. er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten der Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten der Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten der Auftragsverarbeiterin bzw. des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in der Anlage (Anhang „Weisungsbefugnis“ zu § 3) festgelegt.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(7) Auskünfte an Dritte oder die betroffene Person darf die Auftragsverarbeiterin bzw. der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch die Verantwortliche erteilen, es sei denn sie bzw. er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(8) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn sie bzw. er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen der Verantwortlichen nicht erstellt.

(9) Die Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter stellt der Verantwortlichen auf deren Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag der Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(10) Die Verarbeitung der Daten im Auftrag der Verantwortlichen findet ausschließlich auf dem Gebiet *der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) / der*

Bundesrepublik Deutschland statt. Jede Übermittlung von Daten durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage schriftlicher (oder dokumentierter elektronischer) Weisungen der Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem die Auftragsverarbeiterin bzw. der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(11) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter gewährleistet, dass ihr bzw. ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung der Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume der Auftragsverarbeiterin bzw. des Auftragsverarbeiter (z.B. Telearbeit, Heimarbeit, Homeoffice, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen (oder dokumentierten elektronischen) Zustimmung der Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter

(1) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies der Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter stellt der Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern die Auftragsverarbeiterin bzw. der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten unterliegt, sind die Kontaktdaten der/des Datenschutzbeauftragten der Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. Unterliegt die Auftragsverarbeiterin bzw. der Auftragsverarbeiter nicht der Benennungspflicht, teilt er der Verantwortlichen die Kontaktdaten einer Ansprechperson für den Datenschutz mit.

(4) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter informiert die Verantwortliche unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang „Technisch-organisatorische Maßnahmen“ wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine von der Verantwortlichen durchzuführende Prüfung einen Anpassungsbedarf hinsichtlich der von der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen, sind die Anpassungen im Einvernehmen zwischen beiden Parteien umzusetzen.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter wird der Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Sie bzw. er wird insbesondere Überprüfungen/ Inspektionen, die von der Verantwortlichen oder einem anderen von dieser beauftragten Prüferin bzw. Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfende, unabhängige Datenschutzauditierende), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter verpflichtet sich, die Verantwortliche über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Die Verantwortliche kann sich hierzu in den Betriebsstätten der Auftragsverarbeiterin bzw. des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(7) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter stellt der Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die sie für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter hat im Benehmen mit der Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter

(1) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter unterrichtet die Verantwortliche umgehend bei schwerwiegenden Störungen ihres bzw. seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten der Verantwortlichen nach Art. 33 und Art. 34 DSGVO.

(2) Die Verantwortliche ist per E-Mail mit dem Betreff „Meldung eines Datenschutzvorfalls“ (ohne Anführungszeichen) an IT-ServiceDesk@bundesimmobilien.de bzw. telefonisch (+49 (0)228 37787-600) zu unterrichten.

(3) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter sichert zu, die Verantwortliche erforderlichenfalls bei ihren Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für die Verantwortliche darf die Auftragsverarbeiterin bzw. der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum der Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch die Verantwortliche, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat die Auftragsverarbeiterin bzw. der Auftragsverarbeiter sämtliche im Auftrag der Verantwortlichen verarbeitete personenbezogene Daten der Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung der Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist der Verantwortlichen auf Anforderung vorzulegen.

(3) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann sie bzw. er diese zu ihrer bzw. seiner Entlastung bei Vertragsende der Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter darf weitere Auftragsverarbeitende (Subunternehmen) nur nach einem der nachfolgenden Verfahren einsetzen: [Zutreffendes bitte ankreuzen]

- ☐ Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die sie bzw. er im Auftrag der Verantwortlichen gemäß dieser Vereinbarung durchführt, ohne vorherige gesonderte schriftliche (oder dokumentierte elektronische) Genehmigung der Verantwortlichen an ein Subunternehmen untervergeben. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmens zusammen mit den Informationen ein, die die Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der von der Verantwortlichen genehmigten Subunternehmen findet sich im Anhang „Subunternehmen“. Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

- ☐ Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Subunternehmen, die in einer vereinbarten Liste aufgeführt sind. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter unterrichtet die Verantwortliche mindestens vier Wochen im Voraus ausdrücklich in schriftlicher (oder dokumentierter elektronischer) Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmen und räumt der Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Subunternehmens Einwände gegen diese Änderungen erheben zu können. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter stellt der Verantwortlichen die erforderlichen Informationen zur Verfügung, damit diese ihr Widerspruchsrecht ausüben kann.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die die Auftragsverarbeiterin bzw. der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch die Auftragsverarbeiterin bzw. den Auftragsverarbeiter eingeschaltet werden, hat die Auftragsverarbeiterin bzw. der Auftragsverarbeiter sicherzustellen, dass ihre bzw. seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen der Verantwortlichen und der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Der Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist die Verantwortliche berechtigt, auf schriftliche (oder dokumentierte elektronische) Anforderung von der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet die Auftragsverarbeiterin bzw. der Auftragsverarbeiter gegenüber der Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter hat in diesem Falle auf Verlangen der Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter verpflichtet sich, der bzw. dem Datenschutzbeauftragten der Verantwortlichen zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Sie bzw. er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Sie bzw. er wird ihre bzw. seine Beschäftigten anweisen, mit dem bzw. der Datenschutzbeauftragten zu kooperieren, insbesondere deren bzw. dessen Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Haftung und Schadenersatz

Auf Artikel 82 DSGVO wird bezüglich der Haftung und des Rechts auf Schadenersatz verwiesen.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen der Auftragsverarbeiterin bzw. des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Datum, Ort	Datum, Ort
Unterschrift (Verantwortliche)	Unterschrift (Auftragsverarbeiter/in)
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Weisungsbefugnis“ zu § 3 (nach Zuschlagserteilung auszufüllen)

zur Vereinbarung zur Auftragsverarbeitung vom [Datum]
zwischen XXXXXX XXXX
und [Vertragspartner]

Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter hat die Verantwortliche unverzüglich zu informieren, wenn sie bzw. er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten der Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten der Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten der Auftragsverarbeiterin bzw. des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Verantwortlichen:

- *X (Weisungsbefugte/r)*
- *XX (Stellvertreter/in)*
- …

Zum Empfang der Weisungen berechtigte Personen auf Seiten der Auftragsverarbeiterin bzw. des Auftragsverarbeiters:

- *Y (für … Bereich)*
- *YY (für … Bereich)*
- *YYY (Stellvertreter/in)*
- …

Vorgesehene Informationswege, wenn Weisung nach Meinung der Auftragsverarbeiterin bzw. des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt: [Zutreffendes bitte ankreuzen]

- ☐ schriftliche und/oder
- ☐ elektronische und/oder
- ☐ mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Kontaktdaten Datenschutzbeauftragter/Ansprechperson Datenschutz:

Verantwortlicher:	Auftragsverarbeiter/in:
Sven Fischer Ellerstraße 56 53119 Bonn Datenschutz@bundesimmobilien.de	

Anhang „Technisch-organisatorische Maßnahmen (TOM)“

zur Vereinbarung zur Auftragsverarbeitung vom [*Datum*]
zwischen *XXXXX XXXX*
und [*Vertragspartner*]

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation der Auftragsverarbeiterin bzw. des Auftragsverarbeiters
Die Auftragsverarbeiterin bzw. der Auftragsverarbeiter wird ihre bzw. seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Geschäftsprozesskontrolle** Maßnahmen, die sicherstellen, dass die Geschäftsprozesse den Anforderungen der DS-GVO genügen und entsprechend umgesetzt sind.	
2.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	
3.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	
4.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	

Nr.	Maßnahme	Umsetzung der Maßnahme
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	
6.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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.	
7.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Verantwortlichen verarbeitet werden können.	
8.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	
9.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.	

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

(3) Folgende Nachweise werden dieser Vereinbarung angefügt: [Zutreffendes bitte ankreuzen]

- ☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
- ☐ Zertifizierung nach Artikel 42 DSGVO
- ☐ Prüfberichte, Testate etc. unabhängiger Prüfer/innen, bspw. Wirtschaftsprüfer/innen, Auditoren bzw. Auditorinnen, Datenschutzbeauftragte etc.
- ☐ geeignete Zertifizierung durch einen Auditprozess

Anhang „Subunternehmen“ zu § 8

Nach § 8 Abs. 1 S. 2 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 S. 3 der Vereinbarung erklärt sich die Verantwortliche mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung	(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung