

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO

Zwischen

Immobilien Sprinkart
Öschlestr. 52
78315 Radolfzell
Kunden-Nr.: **99872**

– Verantwortlicher, nachfolgend „Auftraggeber“ genannt –

und

Immowelt AG, Nordostpark 3-5, 90411 Nürnberg

– Auftragsverarbeiter, nachfolgend „Auftragnehmer“ genannt –

und gemeinsam als „Parteien“ bezeichnet.

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem Software-/Servicevertrag vom 05.02.2018 mit der Angebots-Nr. 767423 (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DS-GVO mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Art und Zweck, Dauer der Auftragsverarbeitung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nur nach Weisung des Auftraggebers. Der Auftraggeber bleibt gemäß Art. 5 Abs. 2 DS-GVO im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“).

2.2 Die Erhebung, Verarbeitung und Nutzung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Verarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der personenbezogenen Daten und auf die dort bestimmten Kategorien betroffener Personen.

2.3 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2.4 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verwendet die Auftraggeber-Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens.

3.2 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt, wird er den Auftraggeber möglichst zeitnah darauf hinweisen. Außerdem ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

3.3 Soweit der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist, die personenbezogenen Daten auch ohne Weisung des Auftraggebers zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.4 Weisungen des Auftraggebers sind mindestens in Textform (z.B. E-Mail) zu erteilen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform (z.B. E-Mail).

3.5 Sofern gegen den Auftragnehmer wegen eines Verstoßes gegen die DS-GVO Ansprüche auf Zahlung von Schadenersatz gemäß Art. 82 DS-GVO geltend gemacht werden, ohne dass der Auftragnehmer gegen eine vom Auftraggeber erlassene Weisung verstoßen hat, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen Ansprüchen frei. Der Auftraggeber übernimmt hierbei auch die Kosten der notwendigen Rechtsverteidigung des Auftragnehmers einschließlich sämtlicher Gerichts- und Anwaltskosten. Die Freistellungspflicht gilt nicht, soweit eine Weisung rechtswidrig und dies für den Auftragnehmer offensichtlich war oder der Schadenersatzanspruch auf die Verletzung einer speziell den Auftragsverarbeitern auferlegten Pflicht aus der DS-GVO gestützt wird.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Erhebung, Verarbeitung oder Nutzung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und Inhaber aller etwaigen Rechte, die die Auftraggeber-Daten betreffen.

4.3 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.4 Soweit sich der Auftragnehmer gegen einen Anspruch auf Schadenersatz nach Art. 82 DS-GVO, gegen ein drohendes oder bereits verhängtes Bußgeld nach Art. 83 DS-GVO oder sonstige Sanktionen im Sinne des Art. 84 DS-GVO mit rechtlichen Mitteln verteidigen will, erlaubt der Auftraggeber dem Auftragnehmer Details der Auftragsverarbeitung inklusive erlassener Weisungen zum Zweck der Verteidigung offenzulegen.

4.5 Der Auftraggeber unterstützt den Auftragnehmer bei Kontrollen durch eine Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

5.2 Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren, bei der Geltendmachung eines Haftungsanspruchs einer betroffenen Person oder eines Dritten oder bei der Geltendmachung eines anderen Anspruchs im Rahmen des Zumutbaren und Erforderlichen, soweit ein Zusammenhang mit dieser Auftragsverarbeitung besteht.

5.3 Sofern der Auftragnehmer von einer Kontrolle oder Maßnahme einer Aufsichtsbehörde betroffen ist, die sich auch auf diese Auftragsverarbeitung bezieht, hat der Auftragnehmer den Auftraggeber hierüber zu informieren. Dies gilt auch, soweit eine Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

5.4 Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen gemäß Art. 28 Abs. 3 Satz 2 lit. b) DS-GVO schriftlich auf die Vertraulichkeit zu verpflichten und sie zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut zu machen. Dies ist nicht erforderlich, wenn die bei der Verarbeitung von Auftraggeber-Daten beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.5 Sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind, ist der Auftragnehmer verpflichtet, einen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis fachkundigen, für die Aufgaben nach Art. 39 DS-GVO fähigen und zuverlässigen betrieblichen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß Art. 38, 39 DS-GVO und § 38 Abs. 2 BDSG ausübt. Zum Zwecke der direkten Kontaktaufnahme durch den Auftraggeber lassen dessen Kontaktdaten

Datenschutzbeauftragter
Nordostpark 3-5, 90411 Nürnberg
E-Mail: datenschutz@immowelt.de

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mindestens in Textform (z.B. E-Mail) mitgeteilt. Sollte keine Bestellpflicht für einen betrieblichen Datenschutzbeauftragten bestehen, benennt der Auftragnehmer gegenüber dem Auftraggeber mindestens in Textform (z.B. E-Mail) einen Ansprechpartner für datenschutzrechtliche Belange und teilt dem Auftraggeber dessen Kontaktdaten mit. Sollte der Auftragnehmer seinen Sitz außerhalb der EU haben, benennt er gegenüber dem Auftraggeber einen Vertreter nach Art. 27 Abs. 1 DS-GVO in der EU und teilt dem Auftraggeber dessen Kontaktdaten mit.

5.6 Der Auftragnehmer unterliegt der behördlichen Aufsicht nach § 40 BDSG sowie den Bußgeld- und Strafvorschriften in § 42, 43 BDSG sowie in Art. 83 Abs. 4-6 DS-GVO nach Maßgabe von § 41 BDSG.

5.7 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der nach Anlage 2 zu treffenden technischen und organisatorischen Maßnahmen im Rahmen der Kontrollrechte nach Ziffer 8 dieses Vertrages nachzuweisen.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer hat vor Beginn der Verarbeitung der Auftraggeber-Daten die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DS-GVO zu implementieren und während des Vertrags aufrechtzuerhalten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

6.2 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

7. Unterstützung des Auftragnehmers zur Einhaltung der Pflichten des Auftraggebers nach Art. 32 – 36 DS-GVO

7.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
- b) die Unterstützung des Auftraggebers im Falle einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO,
- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht nach Art. 34 DS-GVO gegenüber einem Betroffenen zu unterstützen,
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzungen i. S. d. Art. 35 DS-GVO,
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde nach Art. 36 DS-GVO.

7.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine dem Leistungsumfang angemessene Vergütung beanspruchen.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen Auftraggeber-Daten verarbeitet werden, zu betreten, um sich von der Einhaltung der aus dieser Vereinbarung ergebenden Pflichten, insbesondere der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag, zu überzeugen. Der Auftragnehmer weist dem Auftraggeber auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen nach.

8.2 Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung der Kontrollen nach Ziffer 8.1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

8.3 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

8.4 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 8 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

8.5 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** anstatt einer Vor-Ort-Kontrolle auch durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren nach Art. 42 DS-GVO, die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag zu überzeugen.

9. Unterauftragsverhältnisse

9.1 Der Auftragnehmer darf Unterauftragsverhältnisse (Unterauftragnehmer) hinsichtlich der Verarbeitung oder Nutzung von Auftraggeber-Daten begründen. Zurzeit sind für den Auftragnehmer die in **Anlage 3** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragnehmer. Sofern der Auftraggeber keine Einwände gegen neue Unterauftragnehmer innerhalb von 2 Wochen ab Zugang der Mitteilung über den neuen Unterauftragnehmer erhebt, gilt dessen Einschaltung als durch den Auftraggeber genehmigt.

9.2 Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.3 Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen, was auch in einem elektronischen Format erfolgen kann (z.B. E-Mail). 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 stellt bei jeder Unterbeauftragung sicher, dass die in Art. 28 Abs. 2 und Abs. 4 DS-GVO genannten Bedingungen eingehalten werden.

9.4 Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 8 muss gegenüber dem Unterauftragnehmer grundsätzlich möglich sein. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, von dem Auftragnehmer Auskunft über den datenschutz wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

9.5 Die Regelungen in dieser Ziffer 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird. Der Auftragnehmer stellt in einem solchen Fall die datenschutzrechtliche Zulässigkeit durch geeignete Rechtsinstrumente, beispielsweise EU-Standardvertragsklauseln, sicher.

9.6 Die Weitergabe von Auftraggeber-Daten an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

10. Rechte der Betroffenen

10.1 Die Rechte der durch die Datenverarbeitung betroffenen Personen nach Kapitel 3 DS-GVO (Art. 12-23 DS-GVO) unter Berücksichtigung von Teil 2, Kapitel 2 BDSG (§§ 32-37 BDSG), insbesondere auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch der gespeicherten Auftraggeber-Daten, sind gegenüber dem Auftraggeber geltend zu machen.

10.2 Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks der unter Ziffer 10.1 aufgeführten Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

10.3 Für den Fall, dass eine betroffene Person ihre Rechte im Sinne von Ziffer 10.1 geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche angesichts der Art der Verarbeitung in angemessenem und für den Auftraggeber erforderlichen Umfang mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen.

10.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

11. Rückgabe und Löschung überlassener Daten und Datenträger

11.1 Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrags) oder früher nach Aufforderung durch den Auftraggeber datenschutzgerecht zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Auftraggeber-Daten enthalten, an den Auftraggeber zurückzugeben. Gleiches gilt für Test- und Ausschussmaterial. Dies gilt nicht, sofern nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

11.2 Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.

11.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

12. Verhältnis zum Hauptvertrag

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

13. Geltungszeitraum

Die Auftragsverarbeitung richtet sich bis Ablauf des 24.05.2018 nach den Bestimmungen des § 11 BDSG. Nach Ablauf des 24.05.2018 richtet sich die Auftragsverarbeitung nach den Bestimmungen des Art. 28 DS-GVO.

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 3: Unterauftragnehmer

Anlage 1: Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen Bei Nutzung der Produkte estateOffice und estatePro

Art und Zweck der Verarbeitung	<p>Unterstützung des Auftraggebers bei Fragen und Problemen zur eingesetzten Software per Fernwartung</p> <p>Durchführung von Schulungen und Systemanpassungen bei Terminen vor Ort</p> <p>Durchführung von Online-Schulungen und Systemanpassungen per Fernwartung</p> <p>Zur Lösung technischer Problem werden Daten vom Kunden auf den Servern der Immowelt gespeichert, ausgelesen und anschließend gelöscht.</p> <p>Bei einer Datenmigration werden beim Umstieg auf estateOffice oder estatePro, Daten verändert und dem Auftraggeber im neuen Format zur Verfügung gestellt.</p> <p>Immowelt stellt für die Kommunikation und zur Unterstützung bei der Einhaltung von rechtlichen Vorgaben zwischen Auftraggeber und dessen Endkunden Online-Dienste zur Verfügung. Dazu werden personenbezogene Daten auf die Server der Immowelt übertragen, gespeichert und organisiert und mit Tracking Informationen zurückgeführt.</p> <p>Bei Nutzung von estateMobile stellt Immowelt ein Gateway zur Verfügung, über das der Auftraggeber einen direkten Zugriff über eine mobile Webseite auf seine estateOffice oder estatePro Datenbank erhält. Für die Übermittlung werden die personenbezogenen Daten temporär auf den Servern der Immowelt gespeichert.</p>
Art der personenbezogenen Daten	<p>Adress- und Kontaktdaten</p> <p>Vertragsdaten</p> <p>Bankverbindungs- und Kontodaten</p> <p>Angebotsdaten</p> <p>Leistungs- und Abrechnungsdaten</p> <p>Aktivitätenprotokoll</p> <p>Mitarbeiterdaten</p>
Kategorien betroffener Personen	<p>Interessenten</p> <p>Kunden/Mieter</p> <p>Makler/Vermittler</p> <p>Lieferanten/Dienstleister</p> <p>Mitarbeiter/frühere Mitarbeiter</p>

Bei Nutzung der Produkte estateSmart oder immowelt i-Tool

Art und Zweck der Verarbeitung	<p>Immowelt gewährt dem Auftraggeber ein zeitlich befristetes Nutzungsrecht an der Web-Software zur Vermittlung und Vermarktung von Immobilien. Dazu werden die Daten auf den Servern der Immowelt gespeichert und organisiert.</p> <p>Unterstützung des Auftraggebers bei Fragen und Problemen zur eingesetzten Software per Fernwartung</p> <p>Durchführung von Schulungen und Systemanpassungen bei Terminen vor Ort</p> <p>Durchführung von Online-Schulungen und Systemanpassungen per Fernwartung</p> <p>Bei einer Datenmigration werden beim Umstieg auf estateSmart oder immowelt i-Tool Daten verändert und innerhalb der Anwendung auf den Servern der Immowelt zur Verfügung gestellt.</p> <p>Bei Nutzung von estateMobile stellt Immowelt ein Gateway zur Verfügung, über das der Auftraggeber einen direkten Zugriff über eine mobile Webseite auf seine estateOffice oder estatePro Datenbank erhält. Für die Übermittlung werden die personenbezogenen Daten temporär auf den Servern der Immowelt gespeichert.</p>
Art der personenbezogenen Daten	<p>Adress- und Kontaktdaten</p> <p>Vertragsdaten</p> <p>Bankverbindungs- und Kontodaten</p> <p>Angebotsdaten</p> <p>Leistungs- und Abrechnungsdaten</p> <p>Aktivitätenprotokoll</p> <p>Mitarbeiterdaten</p>
Kategorien betroffener Personen	<p>Interessenten</p> <p>Kunden/Mieter</p> <p>Makler/Vermittler</p> <p>Lieferanten/Dienstleister</p> <p>Kontaktpersonen</p> <p>Mitarbeiter/frühere Mitarbeiter</p>

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Chipkarten-/Transponder-Schließsystem.
- Manuelles Schließsystem für Serverräume.
- Sicherheitsschlösser.
- Schlüsselregelung (Schlüsselausgabe etc.).
- Personenkontrolle beim Empfang für Besucher.
- Protokollierung der Besucher.
- Sorgfältige Auswahl von Reinigungspersonal.
- Einsatz von Wachpersonal.

Zugangskontrolle/Verschlüsselung

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen: Alle IT-Programme laufen auf dem eigenen Server im Rechenzentrum (Housing).

- Zugang ist besonders gesichert (Verschlüsselung, VPN).
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall).
- Zugang zu EDV-Systemen nur mit Benutzererkennung und individuellem Passwort möglich.
- Zugangsberechtigungen werden dokumentiert.
- Passwortsrichtlinie wird über Active Directory durchgesetzt.
- IT-Systeme werden bei wiederholt erfolglosem Anmeldeversuch automatisch gesperrt.
- Funktionale Zuordnung einzelner Endgeräte und Protokollierung der Systemnutzung.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer, zentrale Verwaltung und Steuerung.
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen.
- Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.

Zweckbindungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Logische Mandantentrennung (softwareseitig).
- Festlegung von Datenbankrechten.
- Trennung von Produktiv- und Testsystem.

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

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:

- Übermittlungen personenbezogener Daten sind in Verfahrensübersicht dokumentiert.
- Verschlüsselte Datenübertragung (https) beim Zugriff auf die Online-Anwendungen.
- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum.
- Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN).
- Bei Hardwaretausch werden Festplatten vorher ausgebaut.
- Physische Löschung von Datenträgern vor Wiederverwendung.
- Kontrollierte Vernichtung von Datenträgern mit Protokollierung (physische Vernichtung, zertifizierter Entsorger).
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel).
- Beim physischen Transport: sichere Transportbehälter/-verpackungen.
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.
- Einrichtungen von Standleitungen bzw. VPN-Tunneln.
- Einsatz von Verschlüsselungstechnologie beim E-Mail-Versand. Sichere Aufbewahrung von Datenträgern.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

- Schadschutz.
- Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Unterbrechungsfreie Stromversorgung (USV).
- Klimaanlage in Serverräumen.
- Geräte zur Überwachung von Temperatur in Serverräumen.
- Schutzsteckdosenleisten in Serverräumen.
- Feuer- und Rauchmeldeanlagen.
- Feuerlöschgeräte vor Serverräumen.
- Erstellen eines Backup- & Recoverykonzepts.
- Testen von Datenwiederherstellung.
- Erstellen eines Notfallplans.
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort.
- Regelmäßige Datensicherung.
- Serverräume nicht unter sanitären Anlagen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)

Auftragskontrolle

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Schriftliche Weisungen an den Auftragnehmer.
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.

Datenschutz-Management

Ein Datenschutz-Management-System ist aufgesetzt und wird regelmäßig auf Aktualität geprüft. Das Prinzip "Privacy by Design" ist in die Entwicklungsprozesse integriert.

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. Zur Erstellung von Nutzungsstatistiken werden anonymisierte Nutzerdaten verwendet

Anlage 3: Unterauftragnehmer

Es werden keine Unterauftragnehmer eingesetzt.

Immowelt AG
Nordostpark 3-5
90411 Nürnberg
Deutschland

T +49 911 520 25-20
F +49 911 520 25-25
info@immowelt.de
immowelt.de

Commerzbank Nürnberg
IBAN: DE03 7608 0040 0133 0160 00
BIC: DRESDEFF760

Immowelt AG, Sitz der Gesellschaft: Nürnberg
Vorstand: Carsten Schlabritz (Vorsitzender), Jürgen Roth, Ulrich Gros
Aufsichtsratsvorsitzender: Dr. Andreas Wiele
Amtsgericht Nürnberg, HRB-Nr. 17587, USt-IdNr. DE 132 761 857