Auftragsverarbeitungs-Vereinbarung

Auftraggeber (Verantwortlicher):

Die Immoinvestoren GmbH, Gottlieb-Daimler-Str. 1, 88696 Owingen
(-folgend AG genannt-)

Auftragnehmer (Auftragsverarbeiter):

……., …….
(-folgend AN genannt-)

Präambel

Die Datenübermittlung an „Dritte“ bedarf zwingend einer Rechtsgrundlage. Personen und Stellen, die personenbezogene Daten „im Auftrag“ erheben, verarbeiten oder nutzen (Auftragsverarbeiter) sind aber keine „Dritte“. Die Übermittlung von Daten an den Auftragnehmer stellt daher selbst keine Datenverarbeitung dar mit der Folge, dass die Übermittlung der Daten an den Auftragnehmer und umgekehrt keiner weiteren datenschutzrechtlichen Legitimation bedarf. Die Datenverarbeitung selbst erfolgt datenschutzrechtlich allein durch den Auftraggeber = Verantwortlichen (AG). Somit ist Art. 28 DSGVO als eine eigenständige Befugnisnorm für die Datenverarbeitung anzusehen: Da herbei die Voraussetzungen des Art. 28 DSGVO erfüllt sind, reicht dies für eine rechtmäßige Übertragung der Datenverarbeitung an den Auftragsverarbeiter (AN) aus.

Es liegt somit ein einheitlicher Datenverarbeitungsvorgang vor. Die Datenverarbeitung durch den Auftragsverarbeiter für den Verantwortlichen ist als einheitlicher Vorgang der Datenverarbeitung gem. Art. 4 Nr. 2 DSGVO zu betrachten, dessen Rechtmäßigkeit nach Art. 6 Abs. 1 DSGVO einheitlich zu prüfen ist.

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Der AN verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages. 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).

Dauer der Vereinbarung:

Der Vertrag beginnt wird auf unbestimmte Zeit geschlossen. Kündigungsfrist ist 4 Wochen auf Monatsende. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutz-vorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Der AG überträgt dem AN personenbezogene Daten zum Zweck der Vertriebsbetreuung mit dem Ziel zur abschließenden Vermittlung/Verkauf von Immobilien oder anderer Dienstleistung. Die Übertragung erfolgt u.a. auf elektronischem, fernmündlichen Wege und die Grundlage der Verarbeitung entspricht der Definition von Art. 4 Nr. 2 DSGVO. Die Art der personenbezogenen Daten entspricht der Definition von Art. 4 Nr. 1, 13 - 14 und Art. 15 DSGVO. Die Kategorie der eingehenden personenbezogenen Daten entspricht dem Katalograhmen von Art. 4 Nr. 1 DSGVO.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers (AG)

a) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der AG verantwortlich. Gleichwohl ist der AN verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den AG gerichtet sind, unverzüglich an diesen weiterzuleiten.
b) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen AG und AN abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
c) Der AG ist berechtigt, sich, wie unter u.s. Pos. Nr. 5 festgelegt, vor Beginn der Verarbeitung und so dann regelmäßig in angemessener Weise von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
d) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des AG (Auftraggebers), Weisungsempfänger des AN (Auftragnehmers)

Weisungsberechtigte Personen des AG sind:

- Ingo Roth, Geschäftsleitung
- Matthias Heißner , Prokurist

Weisungsempfänger beim Auftragnehmer sind:

- (Vorname, Name, Organisationseinheit) _____

Für Weisung zu nutzende Kommunikationskanäle:

Beim AG: _____

Beim AN: _____

(jeweils genaue postalische Adresse/ E-Mail/ whats-app/Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5. Pflichten des AN (Auftragnehmers)

a) Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden).
b) Der AG verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des AG nicht erstellt. Er sichert zu, dass die für den AG verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der AN hat über die gesamte Abwicklung der Dienstleistung für den AG insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 - 22 DSGVO durch den AG, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des AG hat der AN im notwendigen Umfang mitzuwirken. Er hat die dazu erforderlichen Angaben bei Anfall unverzüglich an folgende Stelle des AG weiterzuleiten:

  z. Hd. Herrn Ingo Roth, Gottlieb-Daimler-Str. 1, 88696 Owingen

- Der AN wird den AG unverzüglich darauf aufmerksam machen, wenn eine vom AG erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO).
- Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der AN nur nach vorheriger Weisung oder Zustimmung durch den AG erteilen.
- Der AN bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimschutzregeln zu beachten, die dem AG obliegen:
- Der AN verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des AG die Vertraulichkeit zu wahren.
- Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).
- Der AN überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

6. Mitteilungspflichten des AN (Auftragnehmers) bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der AN teilt dem AG unverzüglich Störungen, Verstöße des AN oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutz-verletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

a) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (s.o. Pos. Nr. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der AN dem AG Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der AN dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.
.
Der AN haftet gegenüber dem AG dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den AN im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

a) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

b) Das im Anhang RISKfree beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

10. Vergütung

Die Vergütung bemisst sich nach folgendem Modus:

_____ .

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

12. Vertragsstrafe

Bei Verstoß des AN gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von 5.000 Euro je Einzelverstoß vereinbart.

13. Sonstiges

a) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
b) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
c) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den AG verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
d) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
e) UN-Recht wird ausgeschlossen.
f) Gerichtsstand ist Sitz des AG.

Owingen, den _____

So gesehen und gezeichnet;

_____ _____

(Auftraggeber) (Auftragnehmer)

Anlage:

Anlage RISKfree

Einleitung

Jeder Verarbeitungsvorgang ist im Ausgangspunkt mit Risiken für Rechte und Freiheiten von Betroffenen verbunden. Fremde können sich etwa der Daten bemächtigen und sie im Zweifel zweckentfremden. Aus diesem Grund sieht Art. 32 DSGVO vor, dass vom Verantwortlichen und vom Auftragsverarbeiter die Sicherheit der Verarbeitung gewährleistet werden muss. Dies geschieht mithilfe von technischen und organisatorischen Maßnahmen (sogenannte TOM).

Bei der Bewertung dieser TOM folgt die DSGVO einem anderen Ansatz als das Bundesdatenschutzgesetz: Für die Beurteilung der TOM muss ab 26. Mai 2018 auf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der natürlichen Person abgestellt werden.

Es gilt also ein risikobasierter Ansatz.

Unmittelbar hieraus folgt, dass jedes Unternehmen die eigenen Verarbeitungstätigkeiten risikobasiert bewerten muss. Nur so können angemessene TOM bestimmt werden. Auch benötigt wird die Risikoanalyse auch, um den Aufsichtsbehörden gegenüber nachzuweisen, dass sich überhaupt jemand die nötigen Gedanken gemacht hat. *Außerdem muss bei einem hohen Risiko gegebenenfalls eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchgeführt werden.*

Wie funktioniert das für diese Vereinbarung notwendige Risk-Assessment, welches wir namentlich RISKfree nennen?

Hierzu sind die Verarbeitungstätigkeiten im eigenen Haus zu überblicken. Denn bewertet werden soll schließlich der jeweilige Verarbeitungsprozess. Hierzu werden umfangreiche „Verarbeitungsverzeichnisse“ aufgestellt. Dies wird die Basis diese RISKfree-Analyse sein.

Zur Erledigung der RISKfree-Analayse (= Risikobewertung) sollten zwei wichtige Überlegungen angestellt und entschieden werden:

- Woran soll die Risikobewertung ausgerichtet werden?
- Mit welcher Methode sollen die Risiken beurteilt werden?

Beide Fragen sind schnell beantwortet: Eine rein datenschutzrechtliche Risikoermittlung ist an den Risiken für personenbezogene Daten gruppiert nach Verfahren auszurichten. Die Methode muss es letztlich ermöglichen, das Niveau von Datenschutzrisiken abzubilden.

Man kann es zum Beispiel auf folgende Formel runterbrechen:

Schwere der Auswirkung x Eintrittswahrscheinlichkeit = Risikohöhe

Die Risikobewertung folgt diesen Schritten:

Damit die Schwere der Auswirkung und die Eintrittswahrscheinlichkeit von Verletzungen beurteilen werden kann, ist natürlich zu wissen, über welche Daten und Verarbeitungsvorgänge gesprochen wird, wie diese geschützt sind und welche Risikoquellen es gibt.

Erster Schritt: Einbindung des Management

Die Ergebnisse der Risikoanalyse selbst sollten der Geschäftsführung berichtet werden. Die Art und Weise der nachfolgenden Risikobehandlung muss häufig ohnehin auf dieser Ebene entschieden werden.

Zweiter Schritt: Festlegung der Verantwortlichkeiten

Es sollte ein Projektteam eingesetzt werden und mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.

Dritter Schritt: Internen und externen Kontext festlegen

Die Risikobewertung findet nicht in einem luftleeren Raum statt, sondern muss sich an den bestehenden datenschutzrechtlichen Anforderungen ausrichten. Zu berücksichtigen sind etwa die gesetzlichen Normen und Gerichtsentscheidungen.

Vierter Schritt: Anwendungsbereich festlegen

Hier wird entschieden, was überhaupt der Gegenstand des Risk-Assessment sein soll. In unserem Fall sind dies die Verarbeitungsprozesse im eigenen Unternehmen in Verbindung mit der Zusammenarbeit mit dem Auftragsverarbeiter..

Fünfter Schritt: Identifikation der Datenschutzrisiken

In einem datenschutzrechtlichen Risk-Assessment gilt es vor allem die möglichen Risiken für die Verfügbarkeit, Vertraulichkeit und Integrität zu identifizieren. Das kann

auf unterschiedliche Weise erfolgen; zum Beispiel durch Audits im Interviewformat oder als Brainstorming.

Sechster Schritt: Risikoanalyse

In diesem Schritt werden zunächst die bereits bestehenden Sicherheitsmaßnahmen festgehalten. Danach werden die Bedrohungen und Risikoquellen ermittelt und eine Aufstellung der Auswirkungen von Verletzungen der Datenschutzziele gefertigt. Schließlich gilt es, die Schwere dieser Auswirkungen für die Betroffenen einzuschätzen und die Eintrittswahrscheinlichkeit zu bewerten. Auswirkungen und Eintrittswahrscheinlichkeit müssen verschiedenen Niveaus zugeordnet werden, etwa:

1. vernachlässigbar,

2. eingeschränkt,

3. signifikant und

4. maximal.

Siebter Schritt: Risikobewertung

Der Analyse folgt die Risikobewertung im engeren Sinne. Dabei werden Risikoklassen definiert, zum Beispiel hohes Risiko, Risiko und geringes Risiko. Die Zuordnung erfolgt über das Produkt der Eintrittswahrscheinlichkeit und Schwere der Auswirkungen. Ist beides vernachlässigbar, ergibt sich zum Beispiel das ERGEBNIS 1 (geringes Risiko); sind Eintrittswahrscheinlichkeit und Auswirkungen maximal, ist das ERGEBNIS 10 (hohes Risiko).

Achter Schritt: Bewältigung der Datenschutzrisiken

Sind diese Risiken analysiert und bewertet, können sie auch bewältigt werden, etwa dadurch, dass für risikoreiche Verarbeitungsvorgänge zusätzliche technische Sicherheitsmaßnahmen implementiert werden und damit die Eintrittswahrscheinlichkeit gesenkt wird.