Smart Host

Vertrag zur Auftragsverarbeitung

nach Art. 28 Abs. 6 DSGVO

(Standardvertragsklauseln der EU-Kommission)

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens zwei Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

    1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

    2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

    3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

    4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der

Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

    1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

    2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

    3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679], die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere

Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

Name	Anschrift	Name, Funktion und Kontaktdaten der Kontaktperson	Unterschrift und Beitrittsdatum
OTP Immobilienverwertung GmbH	Gurktaler Weg 6 9546 Bad Kleinkirchheim		

Auftragsverarbeiter:

Name	Anschrift	Name, Funktion und Kontaktdaten der Kontaktperson	Unterschrift und Beitrittsdatum
Smart Host GmbH	Am Kupfergraben 6 A, 10117 Berlin	Julian Leitner Geschäftsführer datenschutz@smart-host.com	

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	● Hotelgäste ● Interessenten für Hotelbuchungen ● Bezieher von Hotel-Kommunikation
Kategorien personenbezogener Daten, die verarbeitet werden	Hotelgäste: ● Stammdaten (Namen, Geburtsdatum) ● Kontaktdaten (E-Mail-Adresse, Telefonnummer) ● Adressdaten (Anschrift/en, Straße/n, PLZ, Ort) ● Kommunikationspräferenzen ● Buchungskanäle (z. B. Reiseveranstalter, Internet-Portal etc.), Buchungshistorie (soweit vorhanden), Gästebewertungen und sonstiges Feedback ● Daten über die Inanspruchnahme der Leistungen des Hotelbetriebs, u.a. Übernachtungen, Zimmer, Datum, übernachtende Personen, gezahlte Preise, Gastronomie, Ratendetails, Zusatzwünsche wie Internet, Kategorie und Ausstattung des Zimmers, sonstige Kommentare etc.. ● Präferenzen und Interessen ● Daten über angefragte Hotelleistungen ● Mitreisende ● Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.) ● Loyalitätsdaten (z.B. Statusniveau, Punkteanzahl) Interessenten: ● Stammdaten (Name) ● Kontaktdaten (E-Mail-Adresse, Telefonnummer) ● Adressdaten (Anschrift/en, Straße/n, PLZ, Ort) ● Kommunikationspräferenzen ● Präferenzen und Interessen ● Daten über angefragte Hotelleistungen, sonstige Kommentare ● Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.) Newsletter-Empfänger: ● wenn zutreffend: Stammdaten (Name) ● Kontaktdaten (E-Mail-Adresse)

	● Kommunikationspräferenzen ● Präferenzen und Interessen ● Daten zur Interaktion mit Hotel-Kommunikation (z.B. Öffnungsevents, Klickevents etc.)
Art der Verarbeitung	Speicherung und Hosting von in der Verantwortung des Verantwortlichen liegenden personenbezogenen Daten im Zuge der Nutzung des Produkts des Auftragsverarbeiters durch den Verantwortlichen. Im Übrigen wird für die Beschreibung des Auftrags auf den zwischen den Parteien geschlossenen (Haupt-)Vertrag über die Nutzung des Dienstes/Produkts des Auftragsverarbeiters verwiesen.
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	Zweck der Datenverarbeitung ist der Betrieb des Dienstes/Produkts des Auftragsverarbeiters für den Verantwortlichen. Der Dienst dient dem Verantwortlichen zur Optimierung seiner Kundenbetreuung. Der vom Verantwortlichen genutzte Dienst des Auftragsverarbeiters setzt die Übermittlung verschiedener Daten, des bzw. aus dem Hotelbetrieb des Verantwortlichen voraus. Der Auftragsverarbeiter nimmt diese Daten entgegen, speichert sie in einer oder mehreren Datenbanken und analysiert sie automatisiert und softwaregesteuert. Die Ergebnisse werden wiederum gespeichert und für den Verantwortlichen im und durch den Dienst nutzbar gemacht.
Dauer der Verarbeitung	Der Auftrag ist entsprechend der Laufzeit des (Haupt-)Vertrages erteilt und kann vom Verantwortlichen und/oder vom Auftragsverarbeiter entsprechend der Regelungen im (Haupt-)Vertrag gekündigt werden. Das Recht der Parteien zur fristlosen Kündigung bei Vorliegen der gesetzlichen Voraussetzungen bleibt hiervon unberührt.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat Smart Host technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO getroffen, die nachfolgend aufgeführt werden.

A. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Vertraulichkeit. Hierunter fallen unter anderem Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Zutrittskontrolle/Gebäudeabsicherung

Unbefugten wird der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, durch folgende Maßnahmen verwehrt:

zu Büroräumen: Die Büroräume von Smart Host befinden sich in Berlin, Am Kupfergraben 6A – 10117 Berlin. In den Räumlichkeiten von Smart Host befindet sich keine kritische IT-Infrastruktur (Serversysteme). Dennoch wird der physikalische Zutritt zu Büroflächen größtmöglich durch Sicherheitsmaßnahmen geschützt:

- Das Gebäude und die Büroräume sind mit einem mechanischen Schließsystem versehen. Die Eingangsbereiche sind stets verschlossen. Die Schlüssel werden ausschließlich vom Management Team ausgegeben und bei den zugriffsberechtigten Personen selbst aufbewahrt. Die Schlüsselausgabe wird protokolliert.
- Betriebsfremde Personen müssen klingeln und sich persönlich anmelden. Sie werden beim Empfang angemeldet und dürfen sich nicht frei, sondern nur begleitet, in den Räumlichkeiten bewegen.
- Das Reinigungspersonal und weitere externe Dienstleister werden sorgfältig ausgewählt.

zu Serverräumen: Smart Host speichert personenbezogene Daten nicht auf eigenen Servern, sondern auf Grundlage einer Auftragsverarbeitung auf Servern des externen Dienstleisters Google (Google Cloud). Als Serverstandorte wurden die Google Rechenzentren Frankfurt, Deutschland (Zone europe-west3) sowie St. Ghislain, Belgien (Zone europe-west1) ausgewählt. Sämtliche Datenschutz- bzw. Sicherheitsmaßnahmen der Server werden von Google bereitgestellt und umgesetzt. Weitere Informationen finden sich unter https://cloud.google.com/security und https://cloud.google.com/terms/data-processingaddendum#appendix-2-security-measures.

Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Smart Host trägt dafür Sorge, 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:

- Zugriffe erfolgen auf Basis eines Berechtigungskonzepts. Es existiert ein definierter Freigabeprozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen. Benutzerrechte und Benutzerzugänge müssen bei der IT beantragt und genehmigt werden. Die Vergabe bzw. Änderungen von Zugriffsberechtigungen werden protokolliert.

- Smart Host gewährleistet, dass ausschließlich Personen Zugriff auf Daten erlangen, die diesen Zugriff zur Aufgabenerfüllung benötigen. Je nach Tätigkeitsgebiet des jeweiligen Mitarbeiters werden abgestufte Berechtigungen vergeben (rollenbasierter Zugriff je nach Abteilung). Hierbei wird stets nach dem Minimalprinzip gearbeitet. Die Anzahl der Systemadministratoren ist auf das Notwendigste reduziert.
- Das Speichern personenbezogener Daten auf mobilen Datenträgern ist untersagt. Alle personenbezogenen Daten werden ausschließlich in der Google Cloud abgelegt.

Zugangskontrolle/Absicherung Systemzugang

Durch folgende Maßnahmen wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Der Zugang zu personenbezogenen Daten ist nur für einen eingegrenzten Kreis an Mitarbeitern möglich. Die dienstlich bereitgestellten Arbeitsgeräte (Client-Rechner) werden nach den gängigen technischen Standards verschlüsselt und sind mit persönlichen Zugangsdaten (User-ID und Passwort) passwortgeschützt. Bei Verlust, Vergessen oder Ausspähen des Passworts setzt der Administrator ein neues Passwort, das der jeweilige Mitarbeiter nach der Erstanmeldung zu ändern hat.
- Eine Übersicht aller Client-Rechner wird unter Aufführung der jeweiligen Seriennummer stets aktuell geführt. Die Client-Rechner werden in den Büroräumen von Smart Host eingesetzt, können aber aufgrund von Geschäftsreisen oder zum Home Office auch außerhalb der Büroräume genutzt werden.
- Benutzerkennungen und Zugänge werden, wenn Mitarbeiter das Unternehmen verlassen, sofort gesperrt, bzw. gelöscht und somit die Zugangsrechte aufgehoben.
- Die Zugangskontrolle gewährleistet des Weiteren der Passwortschutz der Anwendungen und verschiedenen Dienste, die bei Smart Host eingesetzt und zur Verarbeitung personenbezogener Daten genutzt werden.

Fernzugang: Bei Fernzugängen erfolgt die Authentisierung ebenfalls mittels persönlicher Accounts inklusive Passwort-Eingabe. Je nach System ist ein VPN zwingend erforderlich.

Firewall: Die Systeme, auf denen die Daten verarbeitet werden, werden über eine Firewall abgesichert. Die Firewall wird regelmäßig aktualisiert.

Trennbarkeit

Smart Host trägt durch die nachfolgenden Maßnahmen dafür Sorge, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Speicherung erfolgt für jeden Mandanten/Kunden getrennt. Auftragsdaten (Gästedaten) und Vertragsdaten des Auftraggebers (Name, Anschrift) werden ebenfalls voneinander getrennt gespeichert. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke nicht möglich ist. Bei der Datenerfassung wird eine Herkunft hinterlegt. Über Filter in der Software wird sichergestellt, dass nur Daten bearbeitet werden können, die zu einem bestimmten Zweck erhoben wurden. Produktiv- und Testsystem werden strikt getrennt.

B. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Integrität. Hierunter fallen unter anderem Maßnahmen zur Kontrolle der Weitergabe und Eingabe von Daten.

Transport- und Übertragungskontrolle (Sicherheit beim Datentransfer)

Smart Host trägt dafür Sorge, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Datenübermittlung an Dienstleister und andere berechtigte Datenempfänger findet ausschließlich digital und verschlüsselt statt und wird systemseitig dokumentiert. Der Transfer personenbezogener Daten erfolgt durchweg verschlüsselt über E-Mail, verschlüsselter Datei als Mailanhang, per PGP/ S/MIME, VPN, per SFTP sowie mit https/TLS. Auf Kundensysteme wird über verschlüsselte Verbindungen zugegriffen. Die Schlüssel bzw. Zertifikate verwaltet die eigene IT von Smart Host.

Eingabekontrolle

Smart Host gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Alle Eingaben werden vom Auftraggeber selbst vorgenommen oder in Auftrag gegeben.

C. Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Smart Host ergreift Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit.

Verfügbarkeitskontrolle

Smart Host trägt dafür Sorge, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Smart Host betreibt keine eigenen Serverressourcen in eigenen Rechenzentren, sondern greift auf die unter A. aufgeführten Google-Rechenzentren zurück, um eine bestmögliche Verfügbarkeit der eingesetzten Systeme zu gewährleisten. Der unterbrechungsfreie Betrieb der Server wird u.a. durch folgende Maßnahmen gewährleistet:

- Monitoring/Überwachung der Systemaktivitäten durch unsere Mitarbeiter
- Sicherung der Produktivumgebung in regelmäßigen Abständen/Datenspiegelung
- Absicherung der Systeme durch eine unterbrechungsfreie Stromversorgung (USV)
- Einsatz einer mehrschichtigen Virenschutz- und Firewall-Architektur
- Feuer-, Wasser- und Temperaturfrühwarnsysteme sowie Brandschutztüren, Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in den Serverräumen
- getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden
- regelmäßiges Patch-Management
- regelmäßiges Durchführen von Penetrations- und Belastungstests
- regelmäßige Trainings des eingesetzten Personals
- Datensicherung auf Basis eines Backup- und Recovery-Konzepts

Weitere Informationen finden sich unter: https://cloud.google.com/terms/data-processing-addendum#appendix-2security-measures

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Smart Host gewährleistet, dass eingesetzte Systeme im Störungsfall wieder hergestellt werden können.

Auf der Basis eines Backup- und Recovery-Konzepts ist eine kurzfristige Wiederherstellung sichergestellt. Die Wirksamkeit des Konzepts wird durch regelmäßige Kontrollen überprüft.

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

Gemäß Art. 32 Abs. 1 lit. d DSGVO hat Smart Host ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur

Gewährleistung der Sicherheit der Verarbeitung etabliert. Prozesse und Systeme werden regelmäßig auf Datensicherheit und Qualität überprüft.

Auftragskontrolle

Gemäß Art. 32 Abs. 1 lit. d DSGVO, Art. 28 Abs. 1 DSGVO gewährleistet Smart Host, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auswahl eingesetzter (Unter-)Auftragsverarbeiter erfolgt unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich der Datensicherheit. Dort wo erforderlich, werden mit (Unter-) Auftragsverarbeitern, die für Smart Host personenbezogene Daten im Auftrag verarbeiten, schriftliche Verträge zur Auftragsverarbeitung nach Maßgabe von Art. 28 Abs. 3 DSGVO abgeschlossen. Smart Host erteilt den (Unter-)Auftragsverarbeitern Weisungen und übt seine Kontrollrechte stichprobenartig aus. Es wird eine Liste der eingesetzten (Unter-)Auftragsverarbeiter geführt. Diese Liste stellt Smart Host auf Anfrage zur Verfügung.

Incident-Response-Management

Bei Smart Host existiert ein Team, das sich um etwaige Datenschutzvorfälle kümmert. Die Teammitglieder werden regelmäßig zum Umgang mit Datenschutzvorfällen geschult.

Datenschutzmanagement

Smart Host gewährleistet einen Prozess zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen, u.a. durch folgende Maßnahmen:

- Smart Host hat schriftlich einen Datenschutzbeauftragten bestellt. Dieser steht den Mitarbeitern wie Externen in Datenschutzfragen zur Verfügung und wird bei ggf. notwendigen Datenschutzfolgenabschätzungen und Datenschutzvorfällen eingebunden.
- Smart Host führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Verfahren, Verzeichnisse, Verträge, etwaige Datenschutzvorfälle und Behördenanfragen werden zu Dokumentations- und Transparenzzwecken in einem internen Datenschutzmanagementsystem vorgehalten.
- Alle Mitarbeiter werden auf die Vertraulichkeit verpflichtet und mit den Themen Datenschutz und Datensicherheit vertraut gemacht.
- Smart Host überprüft regelmäßig, ob/in welchem Umfang Zugangsrechte noch erforderlich sind.
- Wenn es aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewandt.
- Es existiert eine definierte Vertreterregelung innerhalb von Funktionsgruppen.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme der auf www.smart-host.com/trust abrufbaren Unterauftragsverarbeiter genehmigt.