MUSTER

Vereinbarung zur Auftragsverarbeitung zwischen

der

Landeshauptstadt Hannover, Platz der Menschenrechte, 30159 Hannover, vertreten durch den Oberbürgermeister, im Folgenden „Verantwortliche“ genannt.

und … im Folgenden „Auftragsverarbeiter“

genannt.

Präambel

Diese Vereinbarung dient der Gewährleistung der Einhaltung der Regeln der DatenschutzGrundverordnung – im Folgenden DS-GVO (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).

Abschnitt 1: Verhältnis zum Hauptvertrag

§ 1 Verhältnis zum Hauptvertrag

Diese Vereinbarung ergänzt den das Leistungsverhältnis begründenden Vertrag (Hauptvertrag). Sie ist als Anlage Bestandteil des Hauptvertrages. Bei Widersprüchen zwischen den Vereinbarungen gilt, dass diese Vereinbarung bei den den Datenschutz betreffenden Regelungen Vorrang genießt, während der Hauptvertrag im Übrigen maßgebend ist, insbesondere soweit Hauptleistungspflichten betroffen sind.

Abschnitt 2: Gegenstand der Datenverarbeitung

§ 2 Gegenstand und Dauer der Verarbeitung

Der Auftragsdatenverarbeitungsvertrag (nachfolgend AVV genannt) umfasst Folgendes:

Bereitstellen einer CDE (im Zuge eines Vertrages, nachfolgend CDE-Vertrag genannt). Des Weiteren wird auf den EVB-IT Cloud-Vertrag und die Leistungsbeschreibung verwiesen.

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

Der AVV beginnt mit Vertragsbeginn der CDE Bereitstellung und wird auf unbestimmte Zeit geschlossen. Eine Kündigung des AVV ist während der Laufzeit des CDE-Vertrages nur unter den unten genannten Voraussetzungen möglich. Eine Kündigung des CDE-Vertrages beinhaltet die Kündigung dieser AVV.

Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar

§ 3 Art und Zweck der Verarbeitung

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):

Personenbezogene Daten werden erhoben, organisiert, angepasst, verarbeitet und gespeichert. Die Erhebung, Verarbeitung und Nutzung der Daten erfolgt zur Erstellung von Benutzerkonten und Protokollierung des Datenzugriffs

§ 4 Art der personenbezogenen Daten

Vorname, Nachname, Titel (Unternehmensfunktion), Unternehmen, geschäftl. E-Mail, geschäftl. Telefonnummer, sowie weitere systeminterne Kennungen (z.B. ID)

§ 5 Kategorien der betroffenen Personen

Mitarbeitende der Verantwortlichen sowie externe Personen (Projektbeteiligte eines BIMProjektes) als Nutzer der CDE (Anwender der Software, verwaltende Personen im Kontext der Softwarenutzung, Ansprechpartner des Auftraggebers im Kontext des CDE-Vertrages)

Abschnitt 3: Rahmen der Datenverarbeitung

§ 6 Sitz des Auftragsverarbeiters innerhalb der EU

Der Auftragsverarbeiter versichert, dass er und gegebenenfalls sämtliche weitere Auftragsverarbeiter, die an der Erbringung der Leistung mitwirken, ihren Sitz ausschließlich innerhalb der Europäischen Union haben und sämtliche Datenverarbeitung innerhalb der Europäischen Union erfolgt.

Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 7 Weisungsbefugnis der Verantwortlichen

(1) Die Verantwortliche ist gegenüber dem Auftragsverarbeiter hinsichtlich der Datenverarbeitung weisungsbefugt. Eine Datenverarbeitung erfolgt ausschließlich auf Weisung der Verantwortlichen, es sei denn, den Auftragsverarbeiter trifft eine abweichende Verpflichtung nach dem Recht der Bundesrepublik Deutschland oder der Europäischen Union.

(2) Der Auftragsverarbeiter ist verpflichtet, Weisungen nach Absatz 1 nachvollziehbar zu dokumentieren, diese Dokumentation bis zum Ende des Vertragsverhältnisses aufzubewahren und sie der Verantwortlichen nach Maßgabe des § 11 nach Beendigung des Vertragsverhältnisses anzubieten.

(3) Verarbeitet der Auftragsverarbeiter Daten nach Abs. 1 Satz 2, 2. Alt., so informiert er die Verantwortliche unverzüglich, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

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

(5) Ggf. Liste weisungsberechtigter Personen und Kommunikationswege

[Hier könnte eine Liste mit im Einzelfall weisungsberechtigten Personen bei der LHH eingefügt werden und bestimmte Kontaktdaten (E-Mail, Telefon) festgehalten werden.]

§ 8 Getrennthalten von Daten, Besondere Kennzeichnung

Der Auftragsverarbeiter verpflichtet sich, die im Rahmen der vertragsgegenständlichen Leistung erhobenen Daten logisch getrennt von anderen Daten zu halten und sie mit einer besonderen Kennzeichnung zu versehen, um eine rasche, abschließende Identifizierung zu ermöglichen.

§ 9 Verpflichtung der Mitarbeiter auf Vertraulichkeit

(1) Der Auftragsverarbeiter 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.

(2) Die Verarbeitung von Daten in Privatwohnungen im Rahmen von Tele- oder Heimarbeit ist nur mit Zustimmung der Verantwortlichen gestattet.

§ 10 Nachunternehmer

(1) Dem Auftragsverarbeiter ist es untersagt, im Zusammenhang mit der geschuldeten Leistung weitere Auftragsverarbeiter in Anspruch zu nehmen, sofern die Verantwortliche dies nicht zuvor in allgemeiner oder spezieller Form erlaubt.

(2) Im Fall einer allgemeinen Erlaubnis unterrichtet der Auftragsverarbeiter die Verantwortliche unverzüglich über die Hinzuziehung Dritter.

(3) Der Auftragsverarbeiter ist verpflichtet, vor der Hinzuziehung Dritter angemessene Maßnahmen zum Datenschutz vertraglich festzulegen, sich hinreichende Garantien über die Einhaltung dieser Maßnahmen geben zu lassen und die Einhaltung dieser Maßnahmen periodisch zu kontrollieren. Das Datenschutzniveau muss mindestens dem des vorliegenden Vertrages entsprechen. Der Vertrag ist in Schrift- oder Textform zu schließen. Kontrollen sind zu dokumentieren. Der Auftragsverarbeiter hat die genannten Maßnahmen gegenüber der Verantwortlichen unaufgefordert darzulegen.

(4) Die Weitergabe von personenbezogenen Daten vor Sicherstellung angemessener Datenschutzmaßnahmen nach Abs. 3 ist untersagt.

(5) Zurzeit sind für den Auftragsverarbeiter die in Anlage ..... mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

§ 11 Pflichten bei Vertragsende

(1) Auf Aufforderung der Verantwortlichen, spätestens aber nach Beendigung des Hauptvertrages hat der Auftragsverarbeiter sämtliche Datenbestände, die im Zusammenhang mit dem Leistungsverhältnis stehen, auszuhändigen und sämtliche Kopien

datenschutzgerecht zu löschen. Verlangt die Verantwortliche die datenschutzgerechte Löschung der Daten an Stelle der Herausgabe, so ist der Auftragsverarbeiter alternativ hierzu verpflichtet.

(2) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, hat der Auftragsverarbeiter unbeschadet etwaiger gesetzlicher Aufbewahrungsfristen ebenfalls an die Verantwortliche nach Maßgabe des Abs. 1 zu übergeben.

(3) Der Auftragsverarbeiter ist verpflichtet, auch die Aushändigung von Daten und Dokumentationen aus den Händen von Subunternehmern an die Verantwortliche nach Maßgabe der Absätze 1 und 2 zu gewährleisten.

Abschnitt 4: Technische und Organisatorische Maßnahmen des Auftragsverarbeiters

§ 12 Technische und organisatorische Maßnahmen zum Datenschutz

(1) Der Auftragsverarbeiter gewährleistet für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DS-GVO wie **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** 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. Diese Maßnahmen sollen u. a. sicherstellen, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (**Zweckbindung**), dass Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (**Transparenz**) und dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (**Intervenierbarkeit**). Entsprechend sind auch die Maßnahmenbereiche zu berücksichtigen, die vorrangig der Minimierung der Eingriffsintensität in die Grundrechte Betroffener dienen.

(2) Diese Maßnahmen müssen Folgendes einschließen:

- Ist die Zutrittskontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass kein Unbefugter Zutritt zu Datenverarbeitungsanlagen bekommt, d.h. PC, Zugang zum Netzwerk, Rechenzentrum etc.
    - Beispielmaßnahmen: Schließsystem (Gebäude, aber auch verschließbare Räume/Arbeitsplätze), Alarmanlage, Videoüberwachung, Pförtner
- Ist die Zugangskontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass kein Unbefugter Zugang zu Datenverarbeitungssystemen bekommt, d.h. zur Software.
    - Beispielmaßnahmen: Anmeldeverfahren (Passwortschutz), Anti-VirenSoftware, Firewalls, Desktop-Sperren, Verschlüsselung von Datenträgern
- Ist die Zugriffskontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass jeder nur auf benötigte Daten Zugriff hat.
    - Beispielmaßnahmen: Berechtigungskonzept, Protokollierung, Minimale Anzahl Admins, Aktenvernichter

- Ist die Trennungskontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass zu unterschiedlichen zwecken erhobene Daten, getrennt verarbeitet werden können.
    - Beispielmaßnahmen: Mandantenfähigkeit (Trennung von Kundendaten), Trennung Produktiv- und Testumgebung

- Ist die Weitergabekontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass Daten bei Übertragung/Transport ausreichend geschützt sind.
    - Beispielmaßnahmen: Nutzung Signaturverfahren, verschlüsselte E-Mails, Sorgfalt bei Transportpersonal, Übertragungsprotokolle (TLS, https)
- Ist die Eingabekontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass nachvollziehbar ist, wer wann was gemacht hat. ○ Beispielmaßnahmen: Protokollierung, individuelle Benutzer
- Ist die Verfügbarkeitskontrolle angemessen? Also reichen die Maßnahmen, um zu garantieren, dass Daten vor Verlust/Zerstörung geschützt sind.
    - Beispielmaßnahmen: Festplattenspiegelung, Back-Up-Konzept, Feuer- und Rauchmeldeanlagen, USV, Notfallkonzept
- Ist das Datenschutz-Management angemessen? Also reichen die Maßnahmen, um zu garantieren, dass Datenschutz im Unternehmen gelebt wird.
    - Beispielmaßnahmen: Beschäftigtenschulungen, Vertraulichkeitsverpflichtung, Stellung eines Datenschutzbeauftragten

§ 13 Nachweis[1]

Der Auftragsverarbeiter hat das Bestehen technischer und organisatorischer Maßnahmen nach § 12 vor Vertragsschluss in Form eines Datenschutz- und Datensicherheitskonzepts nebst Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gegenüber der Verantwortlichen nachgewiesen. Die entsprechenden Konzepte sind dieser Vereinbarung als Anlage ……. beigefügt und sind Bestandteil des Vertrages.

Abschnitt 4: Sonstige Pflichten des Auftragsverarbeiters

§ 14 Datenschutzbeauftragter bei dem Auftragsverarbeiter

Der Auftragsverarbeiter benennt gegenüber der Verantwortlichen einen Datenschutzbeauftragten, wenn er gesetzlich zur Bestellung eines solchen verpflichtet ist. Ist der Auftragsverarbeiter nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, so bestellt er einen Verantwortlichen der im Innenverhältnis mit der Verantwortlichen die Aufgaben und Rechte eines Datenschutzbeauftragten übernimmt.

§ 15 Unterstützung bei der Einhaltung von Betroffenenrechten

Der Auftragsverarbeiter unterstützt die Verantwortliche mit geeigneten technischen und organisatorischen Maßnahmen dabei, ihrer Pflicht zur Gewährleistung von Betroffenenrechten nach Kapitel III der Datenschutz-Grundverordnung nachzukommen. Insbesondere gewährleistet der Auftragsverarbeiter Such-, Lösch-, Sperr- und Berichtigungsfunktionen.

§ 16 Pflicht zur Offenlegung von Verletzungen des Datenschutzrechts

Der Auftragsverarbeiter teilt der Verantwortlichen unverzüglich Verletzungen des Schutzes personenbezogener Daten mit. Er informiert die Verantwortliche ebenso unverzüglich über den

---

[1] Es obliegt der Verantwortlichen, vor Vertragsschluss „Garantien" für die zuverlässige Auftragsverarbeitung zu erwirken, Art. 28 Abs. 1. Es läuft darauf hinaus, dass vor Vertragsschluss eine fachkundige Bewertung aufgrund qualifizierter Unterlagen erfolgen muss, ob der Auftragsverarbeiter den Datenschutz gewährleisten kann.

begründeten Verdacht von Verletzungen des Schutzes personenbezogener Daten. Der Auftragsverarbeiter sichert zu, der Verantwortlichen erforderlichenfalls bei ihren Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

§ 17 Unterstützung bei der Gewährleistung der Sicherheit personenbezogener Daten, Inspektionen

(1) Der Auftragsverarbeiter unterstützt die Verantwortliche bei der Gewährleistung der Sicherheit personenbezogener Daten und der Einhaltung der gesetzlichen Vorgaben. Zu diesem Zweck ist er insbesondere verpflichtet, der Verantwortlichen innerhalb angemessener Frist sämtliche Informationen im Zusammenhang mit den Vorschriften der Art. 28-36 DS-GVO zukommen zu lassen.

(2) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass die Verantwortliche - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch von der Verantwortlichen beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.

§ 18 Vertraulichkeit

Der Auftragsverarbeiter sichert der Verantwortlichen Vertraulichkeit im Hinblick auf die vertragsgegenständlichen personenbezogenen Daten, aber auch im Hinblick auf interne Abläufe, Verfahren und technische Einrichtungen der Verantwortlichen zu. Diese Verpflichtung besteht nach Beendigung des Vertrages fort.

§ 19 Haftung

Auf Art. 82 DSGVO wird verwiesen.

Abschnitt 5: Schlussbestimmungen

§ 20 Dauer des Vertragsverhältnisses, außerordentliches Kündigungsrecht

(1) Soweit keine abweichende Regelung getroffen ist, richtet sich die Dauer dieses Vertrages nach der Dauer des Hauptvertrages.

(2) Zusätzlich zu den im Hauptvertrag geregelten Kündigungsmöglichkeiten kann die Verantwortliche den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein nicht nur unerheblicher Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages trotz entsprechender Abmahnung nicht abgestellt wird. Ist der Verstoß schwerwiegend und der Verantwortlichen das Festhalten an dem Vertrag nicht zumutbar, ist eine vorherige Abmahnung entbehrlich.

§ 21 Schrift- bzw. Textformerfordernis

Änderungen dieses Vertrages bedürfen der Schrift- oder Textform. Dies gilt auch für die Änderung des Formerfordernisses selbst.

§ 22 salvatorische Klausel

Sollten Teile dieses Vertrages unwirksam sein oder werden, berührt dies die Wirksamkeit dieses Vertrages im Übrigen oder die Wirksamkeit des Hauptvertrages nicht. Die Parteien verpflichten sich im Fall einer Unwirksamkeit dazu, eine wirksame Regelung zu schließen, die dem Sinn und Zweck der beabsichtigten Regelung entspricht. Dabei Berücksichtigen die Parteien den Geist der Datenschutz-Grundverordnung.

Landeshauptstadt Hannover	Auftragsverarbeiter