

## **VEREINBARUNG ÜBER EINE DATENVERARBEITUNG IM AUFTRAG NACH ART. 28 ABSATZ 3 DER EU DATENSCHUTZGRUNDVERORDNUNG (DS-GVO)**

Anlage zum Vertrag/Auftrag vom

zwischen Auftraggeber

und Auftragnehmer (Auftragsverarbeiter) **EPLASS project collaboration GmbH**

### **Präambel**

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem oben genannten Vertrag/Auftrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag/Auftrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten («Daten») des Auftraggebers verarbeiten.

### **§1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung**

Aus dem Vertrag/Auftrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Datenkategorien, Zwecke und Betroffenenkategorien Inhalt der Auftragsverarbeitung:

#### **■ Art der Daten**

- Identifikationsdaten: Vor- und Nachname, Telefon, Mobiltelefon, E-Mail-Adresse/Adresse
- Personaldaten: Abteilung/Rolle
- Beschäftigtendaten: Keine
- Individuelle Daten:
  - Protokolldaten (Log-in, Änderung der Konfiguration)
  - Kommunikationsdaten und -inhalte (Nachricht, Dateianhang, Versand- und Empfangsdatum)
  - Protokolldaten Web- und E-Mail-Server
- Besondere Arten personenbezogener Daten: Keine
- vom Kunden in die Plattform eingestellte oder versendete Inhalte
  - wie Pläne, Mängel, Bauwerksdaten
  - Nachrichten an Projektbeteiligte

## ■ Art und Zweck der Datenverarbeitung

- Betreiben eines Common Data Environment (CDE) für Bau- und Ingenieurprojekte als SaaS-Provider (Software-as-a-Service) und Erbringung weiterer Services wie Konfiguration, Betreuung des CDE und Schulungen.
- Arten der Verarbeitung sind:
  - Verwaltung von Accounts für die Nutzung der Plattform.
  - Kontaktdaten für die Identifizierung (Rolle, Berechtigung) des Projektraum Teilnehmers
  - Zustellung von Nachrichten
- Betriebssicherheit

## ■ Kategorien betroffener Personen

- vom Kunden in den Projektraum hinzugefügten Teilnehmer
  - Mitarbeiter des Kunden
  - Mitarbeiter von Dienstleister-/Lieferanten des Kunden
  - sonstige vom Kunden hinzugefügte Teilnehmer
- die von der Kommunikation betroffenen oder in den Dateninhalten erfassten Personenkategorien (wie oben und: weitere Beteiligte und externe Kommunikationspartner)

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages/Auftrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

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. Eine Bearbeitung in einem Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in einem Drittland

- ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO);
- wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

- wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DS-GVO)

## §2 Anwendungsbereich und Verantwortlichkeiten

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag/Auftrag und ggf. in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art.4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch den Vertrag/Auftrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag/Auftrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

## §3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer ergreift technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen, insbesondere welche die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen (Anlage 1) bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen

gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
6. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren und zu vergüten, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

## §4 Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## §5 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## §6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber folgende Informationen zur Verfügung vorlegen:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
  - Durchführung von Selbstaudits
  - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. Zertifikat zur Informationssicherheit ISO 27001)
  - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
  - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der

eingerrichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. In diesem Fall werden Auftraggeber und Auftragnehmer einen neuen Prüfer einvernehmlich auswählen.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

## §7 Subunternehmer

1. Der Einsatz von Subunternehmern für die Verarbeitung oder Nutzung personenbezogener Daten als weiteren Auftragsverarbeiter ist zulässig. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Zustimmung zum Einsatz von weiteren Subunternehmern (Art. 28 Nr. 2 DS-GVO). Eine Liste der Subunternehmer liegt als Anlage 2 bei.
2. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine vertraglichen Regelungen in der Vertragskette und datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Erfüllt ein Subunternehmer diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten.
3. Der Auftragnehmer stellt den Auftraggeber auf Nachfrage eine aktuelle Liste der Subunternehmer zur Verfügung. Hierzu teilt der Auftraggeber dem Auftragnehmer eine E-Mail-Adresse mit. Der Auftragnehmer informiert den Auftraggeber über jede Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Subunternehmer. Der Auftraggeber hat die Möglichkeit gegen die Änderung – innerhalb angemessener Frist – Einspruch zu erheben.
4. Nicht als Unterauftragsverhältnisse 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.

## §8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Soweit im Hauptvertrag nicht anders geregelt, gilt deutsches Recht und der Gerichtsstand am Sitz des Auftragnehmers als vereinbart.

## §9 Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, sich selbst oder durch beauftragte Dritte vor Beginn der Datenverarbeitung durch den Auftragnehmer und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen auch vor Ort zu überzeugen.

Der Rhythmus der regelmäßigen Kontrollen orientiert sich an den Erforderlichkeiten des Auftrages. Hierzu weist der Auftragnehmer auf Anforderung die Umsetzung der technischen und organisatorischen Maßnahmen gemäß dieser Vereinbarung und Art. 32 DS-GVO in geeigneter Weise nach.

Der Auftraggeber wird bei Vor-Ort-Kontrollen auf die betrieblichen Abläufe des Auftragsverarbeiters Rücksicht nehmen und Kontrollen mindestens 24 Stunden vorher anmelden. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Durchführung der Kontrollen nach besten Kräften zu unterstützen.

Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung personenbezogener Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise verfügbar zu machen.

Jede Partei trägt grundsätzlich die eigenen Kosten für Kontrollen selbst. Der Aufwand einer Kontrolle ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Für mehrtägige Kontrollen darf der Auftragnehmer eine Vergütung verlangen.

Über jede Kontrolle ist seitens des Auftraggebers ein ausführlicher, schriftlicher Auditbericht anzufertigen und dem Auftragnehmer kostenfrei zu überlassen.

### **§10 Haftung und Schadenersatz**

Soweit im Hauptvertrag nichts anderes vereinbart, haften Auftraggeber und Auftragnehmer gegenüber betroffener Personen entsprechend den gesetzlichen Regelungen.

---

Datum und Unterschrift Auftraggeber

---

Datum und Unterschrift Auftragnehmer

- Anlage 1: Technische und organisatorische Maßnahmen
- Anlage 2: Verzeichnis Subunternehmer