Vertrag zum Datenschutz und zur Datensicherheit
in Auftragsverhältnissen nach Art. 28 und 29 EU-DSGVO

abgeschlossen zwischen

1. **Verantwortliche**

in weiterer Folge auch „für die Verarbeitung Verantwortlicher“ genannt,
und

2. **PlanRadar GmbH**
FN 400573 d
Schottenring 16, DG 1
1010 Wien

in weiterer Folge auch „Auftragsverarbeiter“ genannt, beide Parteien gemeinsam werden auch „Vertragsparteien“ genannt.

1. Anwendungsbereich

1.1. 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 zu gewährleisten.

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 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 erfüllt werden.

2. Unveränderbarkeit der Klauseln

2.1. 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.

3. Auslegung

3.1

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 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 auszulegen.

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

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.

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.

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.

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 die in Anhang II genannten spezifischen Zwecke, 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 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 zuständigen Aufsichtsbehörde die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens 4 Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

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 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 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.

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 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.

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 Verantwort-

liche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 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 Aufsichtsbehörde, 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 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.

A. 10. Verstöße gegen die Klauseln und Beendigung des Vertrages

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – 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 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 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.

Wien, am

Ort, am

_____

PlanRadar GmbH

_____

Kunde

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

Name: …
Anschrift: …

Name, Funktion und Kontaktdaten der Kontaktperson: …
Name, Funktion und Kontaktdaten des Datenschutzbeauftragten:

Auftragsverarbeiter:

PlanRadar GmbH
FN 400573 d
Schottenring 16, DG 1
1010 Wien

Name, Funktion und Kontaktdaten der Kontaktperson:
Name und Kontaktdaten des Datenschutzbeauftragten: Constantin Köck, c.koeck@planradar.com

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Die vom für die Verarbeitung Verantwortlichen zu den Projekten eingeladenen Anwender der Software-as-a-Service Lösung PlanRadar (z.B. Kunden, Sublieferanten, Mitarbeiter)

Kategorien personenbezogener Daten, die verarbeitet werden:

- Kommunikationsdaten (E-Mail, optional Telefonnummer)
- Vertragsstammdaten (Name, E-Mail, Unternehmen)
- Ticketinformationen (Ersteller/in, Erstellungsdatum, Änderungsdatum, Sprachmemos)

Art der Verarbeitung:

- Diese Verarbeitungen umfassen – je nach Bedarf des Anwenders – das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Übermittlung, den Abgleich oder die Verknüpfung, die Einschränkung oder das Löschen von Daten.

Zweck, für den die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Zurverfügungstellung der Software-as-a-Service Lösung PlanRadar für Baudokumentation, Aufgaben- und Mängelmanagement insbesondere zur Vereinfachung der Dokumentation und Kommunikation bei Bau- und Immobilienprojekten. Zu diesem Zweck kann der Anwender über die cloud-basierte Software Daten zu Projekten, Aufgaben, einzelnen Arbeitsschritten und den jeweils daran beteiligten Personen verarbeiten.

Dauer der Verarbeitung:

- Die Dauer der Verarbeitung richtet sich nach dem Hauptvertrag. Darüberhinausgehend kann der für die Verarbeitung Verantwortliche den Vertrag gemäß Punkt 10 kündigen.

Verarbeitung durch Unterauftragsverarbeiter:

- Das Speichern der Daten in der Cloud (Cloud-Hosting) erfolgt durch einen Unterauftragsverarbeiter (siehe Anhang IV). Die Dauer der Verarbeitung richtet sich nach dem Hauptvertrag.

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

A. Zutrittskontrolle

Das Ziel besteht darin, den Zugang zu Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, vor unbefugten Personen zu schützen.

Maßnahme	**Beschreibung**
Alarmanlage	Alarmsysteme zur Sicherung eines Gebäudes vor Einbruch und anderen kriminellen Aktivitäten sind vorhanden. Im Falle eines auslösenden Alarms wird umgehend eine Benachrichtigung an eine zentrale Sicherheitsstelle gesendet, um unverzüglich geeignete Maßnahmen zu ergreifen.
Rechenzentren*	Rechenzentren, Server und Hostsoftwaresysteme sind in unscheinbaren Gebäuden untergebracht. Diese sind mittels physischer Sicherheitsmaßnahmen abgesichert, um unbefugten Zugang sowohl außerhalb des Geländes (durch Zäune und Mauern) als auch innerhalb der Gebäude zu verhindern.
Alarmanlage in den Serverstandorten*	Der Zugang zu Serverstandorten wird über Alarmanlagen abgesichert, die einen Alarm auslösen, wenn die Tür kompromittiert wird.
Automatische Zugangskontrollsysteme in den Serverstandorten*	Der Zutritt zu Serverstandorten wird durch elektronische Zugangskontrollen verwaltet, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
Chipkarten und Ausgaberegelung	Der Schutz vor unbefugtem Zutritt wird durch Chipkarten verwaltet. Ein offizielles Übergabeprotokoll für Chipkarten muss von jedem Mitarbeiter unterzeichnet werden. Die Chipkarten dürfen nicht an andere Personen weitergegeben werden.
Protokollierung der Besucher	Besucher müssen sich stets ausweisen, und sie werden immer von Personal begleitet.
Protokollierung der Besucher in den Serverstandorten*	Besucher sind verpflichtet, sich zu identifizieren und den Registrierungsprozess zu durchlaufen, während sie kontinuierlich von befugtem Personal begleitet werden. Die Genehmigung zur Zutrittsberechtigung erfolgt durch eine befugte Person und wird innerhalb von 24 Stunden widerrufen, sobald ein Datensatz für Mitarbeiter oder Lieferanten deaktiviert wird.
Portier-/Wachdienst	Portier- und Wachdienste überwachen den Zugang zu dem Gebäude.

Portier-/Wachdienst in den Serverstandorten*	Portier- und Wachdienste überwachen den Zugang zu dem Gebäude und sensiblen Bereichen. Ausgebildete Sicherheitskräfte bewachen die Rechenzentren und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.
Videoüberwachung	Die Videoüberwachung ist in den Gebäudebereichen zur Kontrolle des Zutritts installiert.
Videoüberwachung in den Serverstandorten*	Sensible Bereiche werden durch Videoüberwachung kontinuierlich überwacht, um den Zugang zu überwachen.

B. Zugangskontrolle

Das Ziel ist, die Nutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern.

Maßnahme	**Beschreibung**
Benutzerrechte in den Rechenzentren*	Um sicherzustellen, dass ausschließlich autorisierte Benutzer und Administratoren auf alle Systemkomponenten zugreifen können, wird jedem Nutzer eine eindeutige Identifikationsnummer zugewiesen. Die Erstellung, Löschung und Modifikation von Benutzer-IDs, Anmeldedaten und anderen Identifikationsmerkmalen wird zusammen mit einem Zeitstempel protokolliert.
Benutzerprofile	Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet; periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten, wird durchgeführt.
Benutzerprofile in den Rechenzentren*	Der Benutzerzugriff wird erst aktiviert, wenn die Personalabteilung einen entsprechenden Datensatz im HR-System erstellt hat. Prinzip der Minimalberechtigung auf „need-to-know-Basis“. Die gewährten Zugriffsrechte auf IT-Systeme werden quartalsweise von befugten Mitarbeitern überprüft. Zugriffsberechtigungen werden unverzüglich entzogen, wenn sie nicht länger für die Tätigkeiten des Benutzers erforderlich sind.
Passwortvergabe	Für die Erstanmeldung bestehen die Passwörter/Pass-Phrasen aus einem einmaligen Wert und werden unmittelbar nach der ersten Verwendung geändert.
Authentifizierung	Authentifizierung erfolgt durch Benutzername und Passwort. Zusätzlich wurde die Multi-Faktor-Authentifizierung eingeführt, die auf mindestens zwei der folgenden Faktoren basiert (wie PIN-Codes oder biometrische Merkmale).
Passwort- Richtlinien	Die Sicherheitsmaßnahmen umfassen die Implementierung von automatischen Kontosperren nach wiederholten fehlgeschlagenen Anmeldeversuchen und die Aktivierung der

	Zwei-Faktor-Authentifizierung für besonders wichtige Konten.
Passwort-Richtlinien in den Rechenzentren*	Benutzerpasswörter müssen spätestens alle 90 Tage geändert werden. Nur komplexe Passwörter sind erlaubt. Die Änderung des Passworts durch einfache Passwortvariationen, wie das Ändern einer einzigen Stelle, ist nicht gestattet.
Clean-Desk/Clear-Screen-Policy	Alle Mitarbeiter werden angewiesen, sämtliche Dokumente und Unterlagen in abschließbaren Schränken oder Schubladen aufzubewahren, wenn sie ihren Arbeitsplatz verlassen. Es sind automatische Sperrmechanismen für Computer/Laptops/Notebooks bei Verlassen des Arbeitsplatzes oder während Inaktivität aktiviert. Papierdokumente mit vertraulichen Informationen werden vernichtet oder ordnungsgemäß entsorgt. Chip Karten und andere physische Zugriffsmittel werden sicher aufbewahrt und nicht offen sichtbar.
WLAN-Richtlinien	Besucher dürfen nur das spezielle Gäste-WiFi verwenden. Mitarbeiter dürfen ihnen keinen Zugriff auf das Haupt-WLAN-Netzwerk gewähren.
Intrusion Detection/Intrusion Prevention System	Früherkennung von Angriffen, Identifikation von Schwachstellen, Schutz kritischer Ressourcen, Protokollierung und Berichterstattung, Aktualisierung und Wartung sind eingesetzt.
Firewall-Richtlinien	Hardware- und Software-Firewalls sind im Einsatz und dienen als wesentliche Elemente zum Schutz Ihres Netzwerks vor unbefugtem Zugriff, Cyberbedrohungen und potenziellen Sicherheitsverletzungen.
Hardware-Firewall in den Rechenzentren*	Antivirensoftware wurde implementiert, die sowohl über einen E-Mail-Filter als auch über Funktionen zur Malware-Erkennung verfügt.
Software-Firewall in den Rechenzentren*	Die Firewall-Geräte sind so eingestellt, dass sie den Zugang zur Datenverarbeitungsumgebung einschränken und die Sicherheit der Computing-Cluster stärken.

C. Zugriffskontrolle

Die Absicht besteht darin sicherzustellen, dass autorisierte Benutzer eines Datenverarbeitungssystems ausschließlich auf die Daten zugreifen können, für die sie Zugriffsberechtigungen haben, und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahme	**Beschreibung**

Anti-Viren-Software	Die Zugriffskontrolle und somit Schutz vor unbefugter Systembenutzung sind durch Anti-Viren-Software gesichert. Die Software führt täglich eine Überprüfung auf Updates durch.
Verschlüsselung von Datenträgern	Der Schutz vor unbefugter Systembenutzung ist durch Verschlüsselung von Datenträgern gesichert.
Berechtigungskonzept	Die Grundsätze “Least Privilege”, “Need-to-know” und “Segregation of Duties” sind eingehalten.
Systemadministrator	Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten. Anzahl der Administratoren auf das „Notwendigste“ reduziert. Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.
Protokollierung von Zugriffen	Protokollierung aller Zugriffe; enthält Informationen wie Benutzername, Zeitpunkt des Zugriffs, Art des Zugriffs und weitere relevante Details.
Aufbewahrungsfristen	Die Datenaufbewahrungsfristen sind entweder gesetzlich vorgeschrieben oder basieren auf Datenschutzvorschriften.

D. Eingabekontrolle

Der Zweck besteht darin, sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.

Maßnahme	**Beschreibung**
Verarbeitungsverzeichnis	Das Verarbeitungsverzeichnis ist erstellt und regelmäßig überprüft.
Eingabe, Änderung und Löschung von Daten	Protokollierung der Eingabe, Änderung und Löschung von Daten, Revisionssichere E-Mail-Archivierung, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen).
Protokoll- und Log-Dateien	Protokoll- und Log-Dateien ermöglichen die Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Protokoll- und Log-Dateien sind gesichert.

E. Weitergabekontrolle

Die Intention ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dies gegebenenfalls überprüft und festgestellt werden kann.

Maßnahme	**Beschreibung**
Pseudonymisierung	In Fällen, wo es möglich ist, Verwendung von Kennziffern anstelle von Namen.
Standleitungen bzw. VPN-Tunneln	Zugriff auf Produktionsdaten ist auf whitelisted IP's (Zugriff via Virtual Private Networks (VPN) od. Büronetzwerk mit Standleitung) begrenzt.
Verhinderung von unbefugtem Kopieren in den Rechenzentren*	Die Mitarbeiter dürfen keine privaten elektronischen Geräte an Informationssysteme anschließen.
Datenverschlüsselung	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Einsatz von Verschlüsselung. Alle Daten sowohl während der Speicherung (Encryption at Rest) als auch während der Übertragung (Encryption in Transit) sind verschlüsselt, um ein hohes Maß an Datenschutz sicherzustellen.
Löschfristen	Löschungsfristen, sowohl für Daten selbst als auch Metadaten wie Logfiles, sind eingesetzt. Die Daten stehen 30 Tage nach Beendigung des Hauptvertrages zum Download zur Verfügung und werden nach dieser Frist (soweit gesetzlich erlaubt) unwiderruflich gelöscht.
Protokollierung der Vernichtung	Die Protokollierung der Vernichtung bezieht sich auf die Dokumentation und Aufzeichnung von Vorgängen, bei denen Daten entsorgt, gelöscht oder vernichtet werden.
Außerbetriebnahme von Speichergeräten in den Rechenzentren*	Wenn ein Speichergerät am Ende seiner Lebensdauer angelangt ist, wird es demagnetisiert und gemäß branchenüblichen Standards sowie den geltenden Datenschutzgesetzen physisch zerstört.

F. Auftragskontrolle

Das Ziel ist sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich gemäß den Anweisungen verarbeitet werden können.

Maßnahme	**Beschreibung**
Verpflichtung auf das Datengeheimnis	Regelmäßige Mitarbeiterschulungen sind implementiert, um Standardprozesse beim Wechsel oder Ausscheiden von Mitarbeitern zu gewährleisten.

schriftliche Weisungen	Eindeutige Vertragsgestaltung; keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO erfolgt ohne entsprechende Weisung des Auftraggebers.
Vernichtung von Daten nach Beendigung des Auftrags	Löschungsfristen für Daten selbst als auch Metadaten wie Logfiles. Die Vernichtung von Daten nach Beendigung des Auftrags ist sichergestellt.
Sub-Auftragsverarbeiter	Strenge Auswahl der Sub-Auftragsverarbeiter (ISO-Zertifizierung, ISMS) und Sicherstellung, dass die technischen und organisatorischen Maßnahmen auch durch den Unterverarbeitungsvertrag beim Sub-Auftragsverarbeiter eingehalten werden.

G. Verfügbarkeitskontrolle

Das Ziel ist sicherzustellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt sind.

Maßnahme	**Beschreibung**
Unterbrechungsfreie Stromversorgung in den Serverräumen*	Die elektrischen Systeme wurden so konzipiert, um vollständige Redundanz sicherzustellen und ohne Beeinträchtigung des Betriebs gewartet werden zu können. Die redundanten Rechenzentren sind rund um die Uhr, sieben Tage die Woche in Betrieb. Unterbrechungsfreie Stromversorgung (USV-Geräte) gewährleisten im Falle eines Stromausfalls eine kontinuierliche Energieversorgung für kritische Bereiche. Generatoren sind installiert, die im Bedarfsfall die gesamte Anlage mit Notstrom versorgen können.
Klimaanlage in den Serverräumen*	Mitarbeiter und entsprechende Systeme überwachen die Temperatur und Luftfeuchtigkeit in den Rechenzentren, um sicherzustellen, dass sie auf einem geeigneten Niveau gehalten werden.
Feuerlöschgeräte in den Serverräumen*	Einrichtungen zur automatischen Branderkennung und -bekämpfung sind in den Rechenzentren vorhanden. Das Brandmeldesystem nutzt Rauchsensoren in sämtlichen Bereichen der Rechenzentren, einschließlich mechanischer und elektrischer Infrastruktur, Kühlräumen sowie den Räumlichkeiten, in denen sich die Generatoren befinden.
Diebstahlschutz in den Serverräumen*	Sichere Platzierung der Systeme, so dass Schutz vor Diebstahl gewährleistet ist.
Backup und Wiederherstellung	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie. Die Daten sind auch gesichert durch regelmäßigen Test und Wiederherstellungsübungen. Das Backup- und Recoverykonzept wird regelmäßig überprüft und an sich ändernde Anforderungen und Technologien angepasst.

Notfallplan	Die regelmäßige Überprüfung der Notfallpläne erfolgt jährlich, wobei eine nahtlose Integration des Business Continuity Managements gewährleistet ist.
Aufbewahrung von Datensicherung an einem ausgelagerten Ort	Das Backup-System ist georedundant konfiguriert. Auslagerung der Backup in andere Gebäude und andere Brandzonen.
Systemlandschaft	Die Produktion Systemen sind redundant ausgelegt, um den Betrieb aufrechtzuerhalten.
Penetrationstests, Test- und Freigabeverfahren	Software durchläuft Test- und Freigabeverfahren, um Fehler, Bugs und Sicherheitslücken zu identifizieren und zu beheben.
Schutz vor Malware und Patchmanagement	Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen, Anti-Malware-Software, regelmäßige Einspielen von Sicherheitspatches und Updates sind eingesetzt.

H. Trennungskontrolle

Das Bestreben besteht darin, sicherzustellen, dass Daten, die zu verschiedenen Zwecken erfasst werden, separat verarbeitet werden können.

Maßnahme	**Beschreibung**
Logische Mandantentrennung	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähigkeit, Sandboxing.
Trennung von Produktiv- und Testsystem	Test- und Produktivsysteme sind logisch getrennt, um das Risiko eines unbefugten Zugriffs oder einer unbefugten Veränderung der Produktivsysteme zu reduzieren.

I. Kryptographie und Pseudonymisierung

Der Zweck ist sicherstellen, dass Informationen vor unbefugtem Zugriff geschützt sind und während der Übertragung oder Speicherung nicht unbefugt verändert werden.

Maßnahme	**Beschreibung**
Pseudonymisierung	Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.
Verschlüsselung von Datenträgern und Endgeräten	Die Verschlüsselung von Datenträgern (z.B. mobile Festplatten, USB-Sticks etc.) und Endgeräten (PC, Laptop).

J. Datenschutzmanagement

Das Ziel ist die angemessene Zuweisung zentraler Verantwortlichkeiten zur Gewährleistung der Kontrolle über die oben beschriebenen Maßnahmen und die Aufrechterhaltung eines hohen Sicherheitsstandards.

Maßnahme	**Beschreibung**
Datenschutzbeauftragter	Es wurde ein Datenschutzbeauftragter ernannt.
Datenschutzmanagement	Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses, einschließlich regelmäßiger Mitarbeiter-Schulungen und Awareness-Maßnahmen.
Datenschutzfreundliche Voreinstellungen	Die Implementierung von Opt-out statt Opt-in und Privacy by Default/by Design zur Stärkung der Privatsphäre und Sicherheit der Benutzerdaten von Anfang an.
Zertifizierungen	ISO 27001 Zertifizierung sowie die Erklärung der Anwendbarkeit “Statement of Applicability” bieten einen Rahmen zur Identifizierung, Kontrolle und Verringerung der mit der Datensicherheit verbundenen Risiken.
Interne Audits	Sicherheitsüberprüfungen auf Infrastruktur- und Anwendungsebene werden regelmäßig durchgeführt. Es findet ein jährliches internes Audit gemäß ISO 27001 statt.
Externe Audits	Externe Audits werden im Rahmen der ISO 27001 Zertifizierung durchgeführt.
Regelmäßige Überprüfung	Verfahren zur Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen finden regelmäßig statt.
IT-Sicherheit	Incident Response Management, Angriffserkennung, Überwachung und Alarmierung, Assetmanagement, Softwareverwaltung und -verteilung, Benutzerrichtlinien für den Umgang mit Geräten und Verhalten bei der Nutzung von Informationstechnologie sind implementiert.

Anmerkung:

Die mit (*) markierte Stellen betreffen ausschließlich Rechenzentren, die von unserem Unterauftragsverarbeiter, Amazon Web Services, als Cloud-Hosting-Anbieter zur Verfügung gestellt werden.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Amazon Webservices (Amazon Web Services EMEA SARL)
   38 Avenue John F. Kennedy, L-1855 Luxembourg

Beschreibung der Verarbeitung:

Der Unterauftragsverarbeiter wird zum Speichern der Daten in der Cloud (Cloud-Hosting) eingesetzt. Der Serverstandort befindet sich in Frankfurt (AWS Region Europe (Frankfurt), eu-central-1). Das Speichern aller Daten erfolgt innerhalb der Europäischen Union.