

NUTZUNGSBEDINGUNGEN FÜR „PLANIT//PRIMAMCP“

Version: 1.2, Stand: 28. September 2026, PLANIT // TECH

1. Geltungsbereich

- 1.1. Diese Nutzungsbedingungen gelten für alle Verträge über die Nutzung der webbasierten Lösung „PLANIT//PRIMAMCP“ zwischen der PLANIT // TECH GmbH, Jungfernstieg 1, 20095 Hamburg, eingetragen im Handelsregister des Amtsgerichts Hamburg unter HRB 180827 (nachfolgend: „Anbieter“), und dem Kunden.
- 1.2. Das Angebot richtet sich sowohl an Verbraucher im Sinne des § 13 BGB als auch Unternehmer im Sinne des § 14 BGB, juristische Personen des öffentlichen Rechts und öffentlich-rechtliche Sondervermögen. Soweit einzelne Regelungen dieser Nutzungsbedingungen nur für Verbraucher oder nur für Unternehmer gelten, wird dies ausdrücklich kenntlich gemacht.
- 1.3. Gegenüber Unternehmern widersprechen wir der Einbeziehung Allgemeiner Einkaufs- oder Geschäftsbedingungen des Kunden ausdrücklich. Entgegenstehende oder abweichende Bedingungen des Kunden gelten nur, wenn ihrer Geltung ausdrücklich in Textform zugestimmt wurde.

2. Vertragsschluss und Registrierung

- 2.1. Der Vertrag kommt durch Registrierung des Kunden (Angebot) und Annahme durch PLANIT // TECH oder durch sonstige individuelle Vereinbarung zustande. Die Annahme kann insbesondere durch Freischaltung des Kundenkontos, Bereitstellung von Zugangsdaten oder Ermöglichung des Zugriffs auf PLANIT// PRIMAMCP erfolgen.
- 2.2. Der Kunde hat die im Rahmen der Registrierung abgefragten Angaben vollständig und richtig anzugeben und aktuell zu halten.
- 2.3. Die kostenlose Testphase und der kostenlose Tarif stehen je natürlicher Person nur einmal zur Verfügung. Die Registrierung mehrerer Konten durch dieselbe Person, insbesondere unter verschiedenen E-Mail-Adressen oder unter unzutreffenden Namen, um die Testphase erneut in Anspruch zu nehmen oder Nutzungsgrenzen zu umgehen, ist unzulässig.

3. Leistungsgegenstand

- 3.1. PLANIT//PRIMAMCP ist ein sogenannter Legal MCP-Server („Model Context Protocol“) mit folgendem Funktionsumfang:
 - 3.1.1. Schnittstellen-Funktion: Der MCP-Server fungiert als technische Brücke zwischen der vom Nutzer verwendeten Künstlichen Intelligenz (z. B. CoPilot, Claude oder ChatGPT) und den bereitgestellten (Rechts-)Datenquellen des Anbieters.
 - 3.1.2. Datenabruf auf Anfrage: Der MCP-Server führt keine eigenständigen Analysen durch. Er wartet passiv darauf, dass die KI des Nutzers eine spezifische Information anfragt (z. B. die Suche nach einem Urteil). Der Server liefert daraufhin die relevanten Datenfragmente an die KI zurück.

- 3.1.3. Keine Eigenständigkeit: Der MCP-Server ist kein eigenständiges Softwareprogramm zur Rechtsberatung, sondern ein technisches Hilfsmittel, das die Wissensbasis der bestehenden KI des Nutzers situativ erweitert.
- 3.2. Art und Umfang der Leistungen ergeben sich aus dem vereinbarten Tarif und der bei Vertragsschluss geltenden Leistungsbeschreibung. Änderungen während der Vertragslaufzeit richten sich nach Ziff. 3.6.
- 3.3. Nutzungsgrenzen und verfügbare Funktionen, insbesondere Requests, Rate Limits, Seats und Funktionsumfänge, richten sich nach dem vereinbarten Lizenzmodell und der Leistungsbeschreibung. Soweit der vereinbarte Tarif auf Seats basiert, entspricht ein Seat einer Nutzerlizenz, die der Kunde einer Person zuweist; die API-Schlüssel dieser Person nutzen deren Lizenz.
- 3.4. Der Zugriff auf PLANIT//PRIMAMCP erfolgt je nach Tarif und Anwendungsfall insbesondere über API-Schlüssel, OAuth oder sonstige bereitgestellte Authentifizierungsverfahren.
- 3.5. Bei Tarifen mit einer festen Nutzungsobergrenze („Hard Cap“) werden weitere Anfragen nach Erreichen des vereinbarten Kontingents bis zur nächsten Erneuerung des Kontingents oder bis zu einem Tarifwechsel abgelehnt. Eine automatische Mehrverbrauchsabrechnung erfolgt nicht.
- 3.6. Der Anbieter ist berechtigt, PLANIT//PRIMAMCP technisch und funktional weiterzuentwickeln. Gegenüber Unternehmen gilt dies, soweit der vertraglich geschuldete Kernumfang nicht unterschritten wird. Gegenüber Verbrauchern sind Änderungen, die über das zur Aufrechterhaltung der Vertragsmäßigkeit erforderliche Maß hinausgehen, nur aus triftigem Grund und ohne zusätzliche Kosten zulässig. Triftige Gründe sind geänderte gesetzliche oder regulatorische Anforderungen, Sicherheitsrisiken oder erforderliche technische Anpassungen. Verbraucher werden über Änderungen nach Maßgabe der gesetzlichen Vorgaben informiert; ihre gesetzlichen Rechte bleiben unberührt.
- 3.7. Die über PLANIT//PRIMAMCP bereitgestellten Inhalte und Ergebnisse dienen ausschließlich der Information und technischen Weiterverarbeitung. Sie stellen weder Rechtsberatung dar noch ersetzen sie eine rechtliche Prüfung im Einzelfall.
- 3.8. Soweit PLANIT//PRIMAMCP gegenüber einem Verbraucher als digitales Produkt oder digitale Dienstleistung bereitgestellt wird, bleiben die zwingenden gesetzlichen Rechte des Verbrauchers, insbesondere hinsichtlich Bereitstellung, Vertragsmäßigkeit, Aktualisierungen, Mängeln und Änderungen des digitalen Produkts, unberührt.
- 4. Nutzungsrechte**
- 4.1. Der Anbieter behält sich alle Rechte am PLANIT//PRIMAMCP vor, die nicht ausdrücklich durch diese Nutzungsbedingungen gewährt werden.
- 4.2. Der Kunde erhält für die Dauer des Vertrags ein nicht ausschließliches, nicht übertragbares und nicht unterlizenzierbares Recht, PLANIT//PRIMAMCP im vertraglich vereinbarten Umfang für eigene Zwecke zu nutzen.

4.3. Sofern vertraglich nicht abweichend vereinbart, werden die Lizenzen als Nutzerlizenzen vergeben. Ein Lizenzsharing ist nicht gestattet.

4.4. Eine Bereitstellung von PLANIT//PRIMAMCP an Dritte als eigenständiger Dienst, Datenbank oder Konkurrenzprodukt ist unzulässig, soweit nicht ausdrücklich etwas anderes vereinbart ist.

5. Pflichten des Kunden

5.1. Dem Kunden ist es untersagt, die über PLANIT//PRIMAMCP bereitgestellten Inhalte automatisiert (z. B. durch Crawler, Scraper oder Bots) in einem Umfang abzugreifen, der über die gewöhnliche Nutzung im Rahmen einer KI-Interaktion hinausgeht.

5.2. Die Nutzung der bereitgestellten Daten zum Zwecke des Trainings, der Feinabstimmung (Fine-Tuning) oder der Verbesserung eigener KI-Modelle oder Algorithmen des Kunden oder Dritter ist untersagt.

5.3. Der Kunde hat Zugangsdaten, API-Schlüssel und sonstige Authentifizierungsinformationen geheim zu halten und gegen unbefugten Zugriff zu schützen.

5.4. Der Kunde darf technische Schutzmaßnahmen, Nutzungsgrenzen oder Zugriffsbeschränkungen nicht umgehen.

5.5. Der Kunde darf PLANIT//PRIMAMCP nicht rechtswidrig nutzen, keine Rechte Dritter verletzen, keine Schadsoftware einbringen und die Funktionsfähigkeit oder Sicherheit von PLANIT//PRIMAMCP nicht beeinträchtigen.

5.6. Soweit der Kunde personenbezogene Daten in PLANIT//PRIMAMCP eingibt oder über PLANIT//PRIMAMCP verarbeiten lässt, hat er vorab sicherzustellen, dass hierfür eine ausreichende datenschutzrechtliche Rechtsgrundlage besteht.

5.7. Der Kunde bleibt für die inhaltliche und rechtliche Prüfung der über PLANIT//PRIMAMCP erhaltenen Ergebnisse sowie für deren Verwendung im Einzelfall allein verantwortlich.

5.8. Der Kunde stellt sicher, dass die von ihm eingeladenen Nutzer diese Nutzungsbedingungen einhalten; ihr Handeln gilt als Handeln des Kunden.

6. Vergütung und Zahlung

6.1. Die vom Kunden zu zahlende Vergütung ergibt sich aus dem bei Vertragsschluss ausgewählten Tarif und den im Bestellprozess angezeigten Preisangaben. Gegenüber Verbrauchern werden sämtliche Preise als Gesamtpreise einschließlich der gesetzlichen Umsatzsteuer ausgewiesen.

6.2. Das Abrechnungsintervall, die Fälligkeit und die Zahlungsweise ergeben sich aus dem bei Vertragsschluss ausgewählten Tarif und den hierzu im Bestellprozess mitgeteilten Angaben.

6.3. Die Zahlungsabwicklung kann über eingesetzte Zahlungsdienstleister erfolgen.

6.4. Bei nicht nur unerheblichem Zahlungsverzug ist PLANIT // TECH nach erfolgloser Mahnung und Ablauf einer angemessenen Zahlungsfrist berechtigt, den Zugang bis zum vollständigen Ausgleich der offenen Forderungen vorübergehend zu sperren, soweit dies unter Berücksichtigung der beiderseitigen Interessen angemessen ist.

7. Laufzeit, Kündigung, Sperrung

- 7.1. Verträge mit Verbrauchern werden auf unbestimmte Zeit geschlossen, soweit der bei Vertragsschluss ausgewählte Tarif keine Mindestlaufzeit vorsieht. Einen Vertrag ohne Mindestlaufzeit kann der Verbraucher jederzeit mit einer Frist von einem Monat kündigen. Sieht der ausgewählte Tarif eine Mindestlaufzeit vor (insbesondere Jahrestarife), so gilt die im Bestellprozess angegebene Erstlaufzeit, höchstens jedoch zwölf Monate. Der Vertrag kann mit einer Frist von einem Monat zum Ablauf der Erstlaufzeit gekündigt werden. Wird er nicht gekündigt, verlängert er sich auf unbestimmte Zeit; der verlängerte Vertrag kann jederzeit mit einer Frist von einem Monat gekündigt werden. Die Vergütung für den verlängerten Zeitraum richtet sich nach dem dann geltenden Monatspreis des Tarifs, soweit im Bestellprozess nichts anderes angegeben ist. Endet der Vertrag vor Ablauf eines bereits im Voraus bezahlten Zeitraums, weil PLANIT // TECH ordentlich gekündigt oder der Verbraucher aus einem von PLANIT // TECH zu vertretenden Grund außerordentlich gekündigt hat, wird die auf den nicht genutzten Zeitraum entfallende Vergütung anteilig erstattet. Gegenüber Unternehmern wird der Vertrag auf unbestimmte Zeit geschlossen, soweit im vereinbarten Tarif oder durch individuelle Vereinbarung nichts Abweichendes geregelt ist. Der Vertrag kann von jeder Partei mit einer Frist von einem Monat zum Monatsende gekündigt werden.
- 7.2. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.
- 7.3. PLANIT // TECH ist berechtigt, den Zugang vorübergehend ganz oder teilweise zu sperren, wenn konkrete Anhaltspunkte für einen nicht nur unerheblichen Verstoß gegen diese Nutzungsbedingungen, eine Gefährdung der Sicherheit oder Integrität der Systeme, eine rechtswidrige Nutzung oder einen nicht nur unerheblichen Zahlungsverzug vorliegen und die Sperrung unter Berücksichtigung der beiderseitigen Interessen angemessen ist. Soweit dies zumutbar ist und kein dringender Sicherheitsfall vorliegt, wird der Kunde vor einer Sperrung informiert und erhält Gelegenheit, den Grund für die Sperrung innerhalb angemessener Frist zu beseitigen.
- 7.4. Verbraucher können eine Kündigung insbesondere auch über die auf der Webseite bereitgestellte elektronische Kündigungsfunktion erklären. Sonstige gesetzlich zulässige Möglichkeiten zur Erklärung einer Kündigung bleiben unberührt.

8. Datenschutz

Sofern der Anbieter ausnahmsweise personenbezogene Daten als Auftragsverarbeiter im Auftrag des Kunden verarbeitet, gilt ergänzend die als **Anlage 1** beigelegte Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

9. Vertraulichkeit

- 9.1. Beide Parteien behandeln alle ihnen im Zusammenhang mit dem Vertrag bekannt werdenden vertraulichen Informationen der jeweils anderen Partei vertraulich.

- 9.2. Dies gilt nicht für Informationen, die öffentlich bekannt sind, ohne Verstoß gegen eine Geheimhaltungspflicht öffentlich werden, bereits rechtmäßig bekannt waren oder aufgrund gesetzlicher Verpflichtung offengelegt werden müssen.
- 9.3. Soweit der Kunde oder dessen Nutzer Informationen verarbeiten, die einer gesetzlichen oder berufsrechtlichen Verschwiegenheitspflicht unterliegen, gilt ergänzend die als **Anlage 2** beigelegte Vertraulichkeits- und Geheimnisschutzvereinbarung.

10. Gewährleistung und Haftung

- 10.1. Es gelten die gesetzlichen Vorschriften, soweit nachfolgend nichts Abweichendes geregelt ist. Gegenüber Verbrauchern bleiben insbesondere die zwingenden gesetzlichen Rechte im Zusammenhang mit der Bereitstellung digitaler Produkte unberührt.
- 10.2. Der Anbieter haftet für Vorsatz und grobe Fahrlässigkeit. Ferner haftet der Anbieter für die fahrlässige Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht, deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Kunde regelmäßig vertrauen darf. In diesem Fall haftet der Anbieter nur für den vorhersehbaren, vertragstypischen Schaden. Gleiches gilt für Pflichtverletzungen von Erfüllungsgehilfen des Anbieters.
- 10.3. Die vorstehenden Haftungsbeschränkungen gelten nicht bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.
- 10.4. Die vorstehenden Haftungsbeschränkungen gelten auch für die persönliche Haftung der Beschäftigten, Vertreter, Organe und Erfüllungsgehilfen von PLANIT // TECH.

11. Schlussbestimmungen

- 11.1. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss seiner Bestimmungen zum internationalen Privatrecht und des UN-Kaufrechts. Gegenüber Verbrauchern gilt diese Rechtswahl nur insoweit, als dadurch nicht der Schutz zwingender Bestimmungen des Rechts des Staates entzogen wird, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat und dessen Schutzvorschriften ohne die Rechtswahl anwendbar wären.
- 11.2. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dem Vertrag ist Hamburg, sofern der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.
- 11.3. Sollten einzelne Bestimmungen dieser Nutzungsbedingungen ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlagen:

- Anlage 1: Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO)
- Anlage 2: Vertraulichkeits- und Geheimnisschutzvereinbarung

ANLAGE 1: Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO)

Die Nutzung von „PLANIT//PRIMAMCP“ führt regelmäßig nicht zu einer Auftragsverarbeitung im Sinne von Art. 28 DSGVO. Personenbezogene Daten sind nicht typischer Gegenstand der Leistung. Soweit PLANIT // TECH im Rahmen der Nutzung von „PLANIT//PRIMAMCP“ ausnahmsweise personenbezogene Daten im Auftrag des Kunden verarbeitet, gelten hierfür die nachfolgenden Standardvertragsklauseln gemäß Art. 28 Abs. 7 DSGVO. Diese Standardvertragsklauseln gelten ausschließlich, soweit und solange im Einzelfall eine Auftragsverarbeitung vorliegt.

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 (Datenschutz-Grundverordnung) 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.
- 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 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.

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 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.

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.

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 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 personenbezogener 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/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) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 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.

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 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 – 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 und der Verordnung (EU) 2016/679 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): Der Verantwortliche ist derjenige Kunde, der den Vertrag über die Nutzung von „PLANIT//PRIMAMCP“ mit der PLANIT // TECH GmbH abgeschlossen hat. Maßgeblich sind die bei Vertragsschluss bzw. im Kundenkonto hinterlegten Unternehmens- und Kontaktdaten.

Name, Funktion und Kontaktdaten der Kontaktperson: Die vom Kunden im Rahmen der Registrierung oder Vertragsverwaltung benannte Kontaktperson.

Datenschutzbeauftragter: Soweit vom Kunden benannt, der bei Vertragsschluss bzw. im Kundenkonto angegebene Datenschutzbeauftragte.

Auftragsverarbeiter: PLANIT // TECH GmbH

Anschrift: Jungfernstieg 1, 20095 Hamburg, Deutschland

Kontaktperson: Dr. Bernhard Freund (Geschäftsführer)

Datenschutzbeauftragter: datenschutz@planitprima.com

ANHANG II

1. Gegenstand und Dauer der Verarbeitung

Gegenstand: Bereitstellung einer technischen Schnittstelle (MCP-Server) zum Abruf von Fachinformationen und Datenbankinhalten durch das KI-System des Nutzers.

Dauer: Die Verarbeitung erfolgt für die Laufzeit des Hauptvertrages über die Nutzung des MCP-Servers.

2. Art und Zweck der Verarbeitung

Art: Erhebung, Speicherung, Übermittlung und Bereitstellung von Daten im Rahmen von API-Abfragen.

Zweck: Ermöglichung des Zugriffs der Nutzer-KI auf die Wissensdatenbank des Anbieters (Context Window Extension). Der Anbieter verarbeitet Daten nur als technischer Durchleiter, um die Suchanfrage der KI zu beantworten.

3. Kategorien betroffener Personen

Beschäftigte des Nutzers: (z. B. Anwälte, Sachbearbeiter, die das Tool bedienen).

Mandanten/Kunden des Nutzers: (Sofern der Nutzer personenbezogene Daten seiner Mandanten in die Suchanfrage an den MCP-Server aufnimmt).

Dritte: (Personen, die in den vom Nutzer hochgeladenen oder abgefragten Sachverhalten vorkommen).

4. Arten personenbezogener Daten

Identifikationsdaten: (z. B. IP-Adresse des anfragenden Systems, User-ID).

Inhaltsdaten: (Jegliche Daten, die der Nutzer in der Anfrage/im Prompt an den MCP-Server sendet; dies können Namen, Aktenzeichen oder Sachverhaltsschilderungen sein).

Log-Daten: (Zeitpunkt des Zugriffs, übertragene Datenmenge, Fehlermeldungen).

ANHANG III

Technisch-organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Präambel

Die Anwendung „PLANIT//PRIMAMCP“ wird auf von der Hetzner Online GmbH betriebenen Systemen in Deutschland gehostet. Soweit nachfolgend Maßnahmen des Hosting-Anbieters beschrieben sind, beziehen sich diese auf die für PLANIT//PRIMAMCP genutzte Infrastruktur. Soweit nachfolgend Maßnahmen des Auftragsverarbeiters beschrieben sind, beziehen sich diese auf die von PLANIT // TECH für PLANIT//PRIMAMCP eingesetzten anwendungsbezogenen und organisatorischen Sicherheitsmaßnahmen.

Die nachfolgenden Maßnahmen dienen der Gewährleistung eines dem Risiko angemessenen Schutzniveaus im Sinne von Art. 32 DSGVO.

1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

1.1. Zutrittskontrolle

- Rechenzentrum Falkenstein (Hetzner)
 - elektronisches Zutrittskontrollsystem mit Protokollierung
 - Hochsicherheitszaun um den gesamten Datacenter-Park
 - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für sein Colocation Rack)
 - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
 - 24/7 personelle Besetzung der Rechenzentren
 - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
 - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
- Verwaltung (Hetzner)
 - elektronisches Zutrittskontrollsystem mit Protokollierung
 - Videoüberwachung an den Ein- und Ausgängen

1.2. Zugangskontrolle

- Sicherheitsmaßnahmen für Dedicated Server (Hetzner)
 - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
 - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

1.3. Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)

- bei internen Verwaltungssystemen (Hetzner)
 - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
 - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- Für die Anwendung (Auftragsverarbeiter)

- Der Auftragsverarbeiter verwendet Berechtigungskonzepte nach dem Least-Privilege-Prinzip und Need-To-Know-Prinzip mit bedarfsgerechter Ausübung der Zugriffsrechte.
- Administrator-Zugriffe werden protokolliert. Für Administrator-Zugriffe wird eine 2-Faktor-Authentifizierung oder eine vergleichbare Maßnahme verwendet.

1.4. Datenträgerkontrolle

- Rechenzentrum Falkenstein (Hetzner)
 - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht) und dann überprüft.
 - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

1.5. Trennungskontrolle

- Interne Verwaltungssysteme (Hetzner)
 - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
 - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Für die Anwendung (Auftragsverarbeiter)
 - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Insbesondere stellt PLANIT//PRIMAMCP durch anwendungsbezogene Zugriffskontrollen und logische Trennung eine Trennung zwischen den Datenbeständen verschiedener Kunden sicher.

2. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

2.1. Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

- Zugriff auf die Anwendung über nach dem Stand der Technik verschlüsselte Verbindungen (TLS)
- Sorgfältige Auswahl des Personals (Auftragsverarbeiter und Hetzner)
- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen (Auftragsverarbeiter und Hetzner).
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung

2.2. Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

- Protokollierung von Administratorzugriffen seitens des Hosting-Providers (Hetzner).
- Protokollierung von Administratorzugriffen, Benutzerlogins und Änderungen an Daten innerhalb der Anwendung (Auftragsverarbeiter).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

3.1. Verfügbarkeitskontrolle

- bei internen Verwaltungssystemen (Hetzner)
 - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
 - Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
 - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
 - Monitoring aller relevanten Server.
 - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
 - Dauerhaft aktiver DDoS-Schutz.
 - Hetzner stellt angemessene Backups der in der Anwendung verarbeiteten Daten an einem vom Produktivsystem getrennten Ort sicher.
- Für die Anwendung (Auftragsverarbeiter)
 - Regelmäßige Datensicherungen nach internem Backup- und Wiederherstellungskonzept

3.2. Rasche Wiederherstellbarkeit

- Hetzner: Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.
- Auftragsverarbeiter: Durch Backups mit definierten RTO und Wiederanlaufkonzepten wird eine Wiederherstellung der Funktionalität der Anwendung in angemessener Zeit sichergestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Hetzner:
 - Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
 - Incident-Response-Management ist vorhanden.

- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Auftragskontrolle
 - Die Mitarbeiter von Hetzner und des Auftragsverarbeiters werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.
 - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Stand: 7. April 2026

PLANIT // TECH

ANHANG IV

Liste der Unterauftragsverarbeiter

Unterauftragsverarbeiter	Kontaktdaten	Gegenstand der Verarbeitung
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen	Hosting-Dienstleistung
PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH	Jungfernstieg 1, 20095 Hamburg	Technischer und administrativer Support mit möglichem Zugriff auf im Auftrag verarbeitete personenbezogene Daten
Proximit GbR	Beerenweg 6-8 22761 Hamburg	Technischer Support mit möglichem Zugriff auf im Auftrag verarbeitete personenbezogene Daten

Stand: 7. April 2026

PLANIT // TECH

ANLAGE 2: Vertraulichkeits- und Geheimnisschutzvereinbarung

1. Anwendungsbereich

Diese Anlage gilt ergänzend zu den Nutzungsbedingungen für „PLANIT//PRIMAMCP“, soweit der Kunde oder dessen Nutzer Informationen verarbeiten, die einer gesetzlichen oder berufsrechtlichen Verschwiegenheitspflicht unterliegen, insbesondere nach § 203 StGB, § 43a Abs. 2 BRAO, § 43e BRAO oder § 2 BORA.

2. Vertrauliche Informationen

Vertrauliche Informationen im Sinne dieser Anlage sind alle im Zusammenhang mit der Nutzung von PLANIT//PRIMAMCP offengelegten, verarbeiteten oder zugänglich gemachten nicht offenkundigen Informationen, insbesondere mandats-, fall-, personen-, unternehmens- oder geschäftsbezogene Informationen.

3. Verpflichtung von PLANIT // TECH

PLANIT // TECH verarbeitet oder erhält solche Informationen nur, soweit dies für die Bereitstellung und den Betrieb von PLANIT//PRIMAMCP erforderlich ist. PLANIT // TECH verpflichtet die mit der Leistungserbringung befassten Personen zur Vertraulichkeit und beschränkt den Zugriff auf diejenigen Personen, die ihn zur Leistungserbringung benötigen. PLANIT // TECH trifft angemessene technische und organisatorische Maßnahmen zum Schutz vertraulicher Informationen.

4. Einsatz weiterer Personen und Dienstleister

Soweit PLANIT // TECH zur Leistungserbringung weitere Personen oder Dienstleister einsetzt, erfolgt dies nur im erforderlichen Umfang. PLANIT // TECH stellt sicher, dass diese nur im erforderlichen Umfang eingebunden und in angemessenem Umfang zur Vertraulichkeit verpflichtet sind.

5. Offenlegung nur bei rechtlicher Verpflichtung

Eine Offenlegung vertraulicher Informationen an Dritte erfolgt nur, soweit dies gesetzlich vorgeschrieben oder zur Durchsetzung gesetzlicher Rechte zwingend erforderlich ist. Soweit rechtlich zulässig, wird der Kunde hierüber vorab informiert.

6. Eigenverantwortung des Kunden

Der Kunde bleibt dafür verantwortlich, vor einer Eingabe oder Verarbeitung zu prüfen, ob und in welchem Umfang PLANIT//PRIMAMCP für Informationen eingesetzt werden darf, die einer gesetzlichen, vertraglichen oder berufsrechtlichen Verschwiegenheitspflicht unterliegen.

7. Vorrang und Fortgeltung

Soweit diese Anlage strengere Anforderungen an den Schutz vertraulicher Informationen stellt als die Nutzungsbedingungen oder sonstige Vertragsbestandteile, gehen diese vor. Die Verpflichtungen aus dieser Anlage gelten auch nach Beendigung des Vertrags fort, soweit und solange gesetzlich oder berufsrechtlich geschützte Geheimhaltungsinteressen bestehen.