

Auftragsverarbeitungsvereinbarung

zwischen

dem Kunden/Nutzer von PlanAPP-Produkten

- Verantwortlicher –
nachstehend „Kunde“ genannt -

und

der PlanAPP GmbH
Imkerstr. 5
30916 Hannover Isernhagen

- Auftragsverarbeiter –
nachstehend „PlanAPP“ genannt

1. Gegenstand, Umfang, Dauer und Spezifizierung der Datenverarbeitung im Auftrag

- (1) PlanAPP bietet ihren Kunden über die Webseite www.planapp.de Softwarelösungen zum Gebrauch über das Internet. Einzelheiten der Vertragsbeziehung zwischen dem Kunden und PlanAPP ergeben sich aus den jeweils vertragsgegenständlichen Angeboten und Leistungsbeschreibungen von PlanAPP und den hierfür gültigen und unter www.planapp.de abrufbaren PlanAPP Nutzungsbedingungen sowie ggf. ergänzend anwendbaren weiteren Vertragsbedingungen, insbesondere Teilnahmebedingungen zum Benchmarking-Programm von PlanAPP. Diese Auftragsverarbeitungsvereinbarung umfasst alle Tätigkeiten, die PlanAPP gemäß entsprechender Angebote, Nutzungs- bzw. Vertragsbedingungen und ggf. etwaiger individueller Einzelvereinbarungen (nachstehend einheitlich „Hauptvertrag“) für den Kunden erbringt und die eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO darstellen. Dies gilt auch, soweit die jeweiligen, den Hauptvertrag bildenden Angebote, Leistungsbeschreibungen, Nutzungs- und sonstigen Vertragsbedingungen nicht ausdrücklich auf diese Auftragsverarbeitungsvereinbarung Bezug nehmen.
- (2) Umfang und Dauer der Auftragsverarbeitung sowie Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten richten sich nach dem Hauptvertrag.
- (3) Der Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten umfasst Daten des Kunden und derjenigen seiner Mitarbeiter, die Produkte von PlanAPP als registrierte „Named User“ verwenden. Hierüber hinaus ermöglicht bzw. erfordert die Nutzung der PlanAPP-Produkte ggf. die Verarbeitung von Personenstammdaten, Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten sowie Planungs- und Steuerungsdaten. Auch die Kategorien der durch die Verarbeitung betroffenen Personen richten sich nach dem Hauptvertrag und umfassen Daten der die PlanAPP-Software betreffenden Nutzerdaten (Daten des Kunden und dessen Mitarbeitern) sowie ggf. Daten von Abnehmern, Lieferanten und sonstigen Geschäftspartnern des Kunden.
- (4) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Die Verlagerung in ein Drittland ist PlanAPP auch ohne Zustimmung des Kunden gestattet, jedoch nur sofern die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (5) Unberührt von dieser Vereinbarung bleiben auf Gesetz oder Einwilligung beruhende Rechte von PlanAPP zur Verarbeitung personenbezogener Daten, die PlanAPP nicht im Auftrag des Kunden i.S.d. Art. 28 DSGVO verarbeitet.

2. Pflichten und Rechte des Kunden

- (1) Der Kunde ist im Rahmen dieser Vereinbarung zur Auftragsverarbeitung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an PlanAPP sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich («Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung und die Beschreibung der betroffenen Daten.
- (2) Der Kunde hat PlanAPP unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.
- (3) Der Kunde nennt PlanAPP bei Bedarf den Ansprechpartner für im Rahmen dieser Vereinbarung zur Auftragsverarbeitung anfallende Datenschutzfragen.
- (4) Weitere Pflichten und Rechte des Kunden ergeben sich aus den nachfolgenden Regelungen dieser Vereinbarung zur Auftragsverarbeitung und der DSGVO und des BDSG sowie ggf. weiter anwendbaren gesetzlichen Bestimmungen.

3. Weisungen

- (1) PlanAPP darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor. PlanAPP nimmt Weisungen des Kunden in schriftlicher Form sowie über die hierfür von PlanAPP angebotenen elektronischen Formate entgegen. Mündliche Weisungen sind durch den Kunden unverzüglich schriftlich oder in einem hierfür von PlanAPP angebotenen elektronischen Format zu bestätigen.
- (2) PlanAPP informiert den Kunden unverzüglich, wenn PlanAPP der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. PlanAPP darf die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.
- (3) Sind die Weisungen des Kunden nicht vom vertraglich vereinbarten Leistungsumfang umfasst, werden diese als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt PlanAPP dem Kunden mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist PlanAPP die Umsetzung der Weisung nicht zumutbar, so ist PlanAPP berechtigt, die Verarbeitung zu beenden. Im Übrigen gelten die Inhalte und Bestimmungen des Hauptvertrags.

4. Vertraulichkeit

PlanAPP gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. PlanAPP setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden oder die einer angemessenen gesetzlichen Verpflichtung zur Berufsverschwiegenheit unterliegen.

5. Technisch-organisatorische Maßnahmen

- (1) PlanAPP gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. PlanAPP ergreift in ihrem Verantwortungsbereich alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen.
- (2) Vorbehaltlich der Bestimmungen der nachfolgenden Ziff. 6 Abs. 3 ergeben sich die jeweils aktuell geltenden technischen und organisatorischen Maßnahmen ergeben sich aus **Anlage A**. Der Kunde informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung und anschließend in regelmäßigen Abständen über diese technischen und organisatorischen Maßnahmen. Der Kunde trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
- (3) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt PlanAPP vorbehalten, sofern das Schutzniveau nach DSGVO nicht unterschritten wird.

6. Weitere Auftragsverarbeiter

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die PlanAPP z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. PlanAPP ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

- (2) Der Kunde erteilt PlanAPP die allgemeine Genehmigung, Unterauftragnehmer (weitere Auftragsverarbeiter) im Sinne des Art. 28 DSGVO in Anspruch zu nehmen.
- (3) Von der Genehmigung nach Abs. 2 umfasst ist insbesondere die gegenwärtige Einschaltung der
 - EDV.de Systemhaus GmbH & Co. KG, Imkerstr. 5, 30916 Hannover Isernhagen (www.edv.de).Von der Genehmigung des Kunden umfasst ist überdies, dass sich die EDV.de Systemhaus GmbH & Co. KG zur Auftragsverarbeitung gegenüber PlanAPP wiederum ihres gegenwärtigen Auftragsverarbeiters
 - DATEV eG, Paumgartnerstraße 6-14, 90429 Nürnberg (www.datev.de)bedient. Die von der DATEV jeweils aktuell geltenden technischen und organisatorischen Maßnahmen im Sinne der Ziff. 4 kann der Kunde unter www.datev.de/info-db/1000562 einsehen.
- (4) PlanAPP informiert den Kunden, wenn PlanAPP eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Kunde kann gegen derartige Änderungen Einspruch erheben. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 4 Wochen nach Zugang der Information über die Änderung gegenüber PlanAPP zu erheben. Im Fall des Einspruchs kann PlanAPP nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung PlanAPP nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunden innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.
- (5) Erteilt PlanAPP Aufträge an weitere Auftragsverarbeiter, so obliegt es PlanAPP, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

7. Unterstützung des Verantwortlichen (Kunden)

- (1) Zur Erfüllung der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person unterstützt PlanAPP den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.
- (2) PlanAPP unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen den Kunden bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.
- (3) PlanAPP ist berechtigt, für die Leistungen nach Abs. 1 und 2 eine angemessene Vergütung und den Ersatz angemessener Aufwendungen vom Kunden zu verlangen.

8. Umgang mit den Daten nach Abschluss der Erbringung der Verarbeitungsleistungen

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht PlanAPP nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach deutschem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt.

9. Informationen und Überprüfungen

- (1) PlanAPP stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen - einschließlich Inspektionen -, die vom Kunden oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und wirkt daran mit. Sofern hierbei die Kenntnisnahmemöglichkeit von vertraulichen Informationen besteht, ist PlanAPP berechtigt, eine Verschwiegenheitserklärung vom Kunden und von diesem beauftragten Prüfer zu verlangen.
- (2) Das Inspektionsrecht des Kunden hat das Ziel, die Einhaltung der einem Auftragsverarbeiter obliegenden Pflichten gemäß der DSGVO und dieses Vertrages zu überprüfen. Der Nachweis soll primär durch unabhängige Prüfberichte und Zertifizierungen erbracht werden. Sofern der Kunde auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass diese Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung des Kunden dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen. Sofern solche Vor-Ort-Kontrollen durchgeführt werden, sind diese als Stichprobenkontrollen der für die Durchführung der Auftragsverarbeitung relevanten Bereiche auszugestalten und PlanAPP rechtzeitig im Voraus, in der Regel (Ausnahme z.B. bei besonderen Vorfällen) mindestens jedoch 14 Kalendertage, schriftlich anzumelden. Das Gleiche gilt für anlasslose Vor-Ort-Kontrollen. Die Ausübung des Inspektionsrechts darf den Geschäftsbetrieb von PlanAPP nicht über Gebühr stören oder missbräuchlich sein.
- (3) PlanAPP ist berechtigt, für Inspektionen eine angemessene Vergütung und den Ersatz angemessener Auswendungen vom Kunden zu verlangen.

10. Gegenseitige Unterstützung

Im Fall des Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

11. Anonymisierungsvereinbarung

- (1) PlanAPP hat das Recht die von dieser Vereinbarung umfassten personenbezogenen Daten zu anonymisieren und vorher die für die Anonymisierung erforderlichen Verarbeitungsschritte durchzuführen (bzw. durch weitere Auftragsverarbeiter durchführen zu lassen), auch soweit dies nicht Gegenstand des Hauptvertrags ist. Unter Wahrung der Anonymität kann PlanAPP alle so entstandenen Daten für eigene Zwecke wie die Erstellung von Betriebs- oder Branchenvergleichen oder sonstige Zwecke mit volks- bzw. betriebswirtschaftlichem Informationscharakter, statistische Auswertungen, Benchmarking, Produktverbesserungen, Produktneuentwicklungen und weitere vergleichbare Zwecke verarbeiten und nutzen. Dies umfasst auch eine anonymisierte Weitergabe an PlanAPP-Anwender und Dritte, insbesondere an Verbände, Organisationen oder Forschungseinrichtungen sowie für Publikationen. Der ursprüngliche Datenbestand ist von dieser Anonymisierung nicht betroffen.
- (2) Der Kunde hat das Recht, der vorstehenden vertraglichen Regelung des Absatzes 1 zu widersprechen, ohne dass dies Auswirkungen auf die übrigen Regelungen dieser Vereinbarung hat. Von einem entsprechenden Widerspruch unberührt bleiben auch Rechte und Pflichten von PlanAPP nach dem Hauptvertrag, insbesondere soweit dieser auf die Datenverwendung für Zwecke des Benchmarkings gerichtet ist.

12. Vereinbarung weiterer Vertragszwecke

- (1) PlanAPP ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zum Zweck der Fehlerbehebung, Qualitätssicherung und Weiterentwicklung in dem PlanAPP-Produkt und etwaigen neueren Versionen entsprechender Produkte, in dem die Daten gespeichert sind bzw. ggf. künftig gespeichert werden - einschließlich entsprechender Entwicklungs- und Testversionen sowie entsprechenden, angemessen gesicherten Umgebungen - , zu verarbeiten (bzw. Unterauftragnehmer verarbeiten zu lassen). PlanAPP berücksichtigt auch in derartigen Verarbeitungsprozessen, dass vom Kunden gelöschte oder zur Löschung angewiesene Daten nicht mehr verarbeitet werden.
- (2) PlanAPP ist berechtigt, die von dieser Vereinbarung umfassten personenbezogenen Daten zu verarbeiten,

- a) soweit sie dies für die Gewährleistung der Netz- und Informationssicherheit als unbedingt notwendig und verhältnismäßig erachtet,
- b) soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit dem vereinbarten Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.
- Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern ("Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

13. Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen von PlanAPP - sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann, und bedürfen des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (2) Sollten Bestimmungen des Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, oder sollte sich in dem Vertrag eine Regelungslücke befinden, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt vorbehaltlich der Regelung in § 306 Abs. 2 BGB diejenige wirksame Bestimmung als vereinbart, die dem wirtschaftlichen Sinn und Zweck der undurchführbaren Bestimmung am Nächsten kommt. Im Falle einer Regelungslücke gilt diejenige Bestimmung als vereinbart, die dem entspricht, was nach dem wirtschaftlichen Sinn und Zweck dieses Vertrages vereinbart worden wäre, hätten die Vertragspartner die Angelegenheit von vornherein bedacht.
- (3) Es gilt deutsches Recht. Gerichtsstand ist Sitz von PlanAPP.
- (4) Bei etwaigen Widersprüchen gehen Regelungen dieser Auftragsverarbeitungsvereinbarung in ihrem Anwendungsbereich den Regelungen des Hauptvertrages vor.
- (5) Soweit in dieser Vereinbarung nichts anderes bestimmt ist, gelten die Bestimmungen des Hauptvertrages auch für diese Vereinbarung. Die anwendbaren Nutzungs- und Teilnahme- und ggf. weiteren Bedingungen von PlanApp sind abrufbar unter <https://planapp.de/downloads/>.

Anlage – Technisch-organisatorische Maßnahmen

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

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Als Auftragsverarbeiter trifft PlanAPP zusätzlich zu Maßnahmen, die sich aus dem jeweiligen Hauptvertrag oder durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine Maßnahmen zur Pseudonymisierung.

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

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

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

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

Datenschutz-Management;

Incident-Response-Management;

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.