HOLZPLANER24

Vertrag über die Auftragsverarbeitung personenbezogener Daten

EU/EWR-Fassung | Stand 17.10.2026 | Version AVV-2026-10-17-EU-3

AUFTRAGNEHMER	AUFTRAGGEBER
Sascha Zeiser **SZ Digital Lab** Niedereichstraße 8 77694 Kehl Deutschland E-Mail: kontakt@sz-digital-lab.de vertreten durch Sascha Zeiser *im Folgenden: Auftragnehmer*	**[Unternehmen / Name des HOLZPLANER24-Kunden]** **[Anschrift]** [PLZ Ort] [Land] [E-Mail] vertreten durch [Name / Funktion] *im Folgenden: Auftraggeber*

Diese Vereinbarung konkretisiert die Auftragsverarbeitung gemäß Art. 28 DSGVO für die Nutzung der webbasierten B2B-SaaS HOLZPLANER24.

1. Einleitung, Geltungsbereich, Definitionen

1.1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag im Sinne des Art. 28 der EU-Datenschutzgrundverordnung (im Folgenden „DSGVO“).

1.2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

1.3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1. Der Auftragnehmer übernimmt folgende Verarbeitungen:

Die Erhebung/Erfassung, Speicherung, Organisation, Verwendung, Auswertung, Bereitstellung, Berichtigung, Exportierung und Löschung personenbezogener Daten von Kunden, Interessenten, Ansprechpartnern und berechtigten Zugangsinhabern des Auftraggebers im Rahmen der webbasierten SaaS „HOLZPLANER24“.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden SaaS-Nutzungsvertrag „HOLZPLANER24 (B2B)“ in der bei Vertragsschluss geltenden Fassung (im Folgenden „Hauptvertrag“).

2.2. Die Verarbeitung beginnt mit Aktivierung des HOLZPLANER24-Kundenkontos bzw. mit Beginn des Hauptvertrags und erfolgt bis zur Beendigung dieses Vertrags oder des Hauptvertrags sowie der anschließenden Rückgabe bzw. Löschung nach den vereinbarten Regelungen.

3. Art und Zweck der Datenverarbeitung

3.1. Der Auftragnehmer erbringt digitale Dienstleistungen und erhält unter gewissen Umständen Zugriff auf den elektronischen Bestand an personenbezogenen Daten und Datensätzen von Kunden des Auftraggebers.

3.2. Die Verarbeitung durch den Auftragnehmer erfolgt in der Art der Erfassung, des Auslesens, des Zuordnens, des Abgleichs, der Organisation, Auswertung und Aufbereitung von Datensätzen des Auftraggebers.

Der Auftraggeber ist ein gewerblich tätiger Betrieb (insbesondere Brennholzhandel bzw. holzwirtschaftlicher Dienstleistungsbetrieb), der HOLZPLANER24 zur Organisation seiner betrieblichen Abläufe nutzt.

3.3. Die Verarbeitung dient der digitalen Kunden- und Interessentenverwaltung, Auftrags- und Terminverwaltung, Lager-/Bedarfsorganisation, Rechnungserstellung und -verwaltung, Auswertung, Bearbeitung von Händleranfragen sowie dem Datenexport. Soweit der Auftraggeber optionale Drittanbieter-Schnittstellen aktiviert, umfasst die Verarbeitung außerdem den vom Auftraggeber veranlassten Datenaustausch mit eigenen Konten bei Buchhaltungs-, Kontakt-, Kalender- oder vergleichbaren Diensten. Bei der optionalen Google-Kontakte-Verbindung umfasst dies den lesenden Import bzw. Abgleich der vom Auftraggeber ausgewählten Kontakte oder Kontaktgruppen/Labels über die Google People API; eine Schreibberechtigung zurück zu Google ist nicht Bestandteil dieser Funktion. Die Verarbeitung erfolgt im Interesse des Auftraggebers an einer strukturierten, effizienten und nachvollziehbaren Organisation seiner Geschäftsabläufe. Bei der optionalen KI-Beleganalyse umfasst die Verarbeitung nach bewusstem Start durch den Nutzer die Übermittlung des zuvor im Browser ausgelesenen Belegtextes an die serverseitig angebundene OpenAI-API zwecks Erkennung und Erstellung prüfpflichtiger Vorschläge; Original-Belegdateien werden dabei nicht an OpenAI übermittelt. Die KI-Bedienhilfe verarbeitet auf Anfrage die eingegebene Bedienungsfrage sowie einen begrenzten Seiten-/Themenkontext, soweit dieser als Verarbeitung im Auftrag zu beurteilen ist. Eine eigenständige betriebliche Buchung durch die KI erfolgt nicht.

3.4. Es werden folgende Kategorien personenbezogener Daten verarbeitet:

- Stamm- und Identifikationsdaten (z. B. Name, Firma, Ansprechpartner)
- Kommunikations- und Adressdaten (Anschrift, Liefer-/Rechnungsanschrift, E-Mail-Adresse, Telefonnummer)
- Nutzer- und Zugangsdaten der HOLZPLANER24-Zugangsinhaber (z. B. E-Mail-Adresse, Benutzerkennung, Rolle sowie Anmelde- und Protokolldaten; Passwörter werden nicht im Klartext gespeichert)
- Auftrags-, Leistungs-, Liefer- und Rechnungsdaten (z. B. Produkte/Leistungen, Mengen, Termine, Preise, Rechnungsnummern, Zahlungsstatus; keine Zahlungsinstrument- oder Zugangsdaten)
- bei optionaler Google-Kontakte-Verbindung: vom Auftraggeber ausgewählte Kontakt- und Zuordnungsdaten sowie technische Ressourcen-/Verbindungskennungen, soweit sie für den lesenden Import und die Synchronisation erforderlich sind
- bei weiteren optionalen Drittanbieter-Schnittstellen: die jeweils vom Auftraggeber zur Übertragung oder zum Abruf freigegebenen Kunden-, Kontakt-, Rechnungs-, Beleg- und Zuordnungsdaten sowie technische Verbindungs- und Mapping-Kennungen; Zugangsdaten, API-Tokens oder vergleichbare Geheimnisse werden nur verarbeitet, soweit dies für die jeweilige Verbindung erforderlich ist
- Anfrage-, Notiz- und Protokolldaten sowie technische Metadaten, soweit sie für Betrieb, Sicherheit und Nachvollziehbarkeit der SaaS erforderlich sind
  - bei aktiver optionaler KI-Nutzung: aus Belegen extrahierte Texte, gegebenenfalls mit personenbezogenen Lieferanten-/Rechnungs-/Leistungsangaben, sowie eingegebene Bedienungsfragen und der begrenzte Seiten-/Themenkontext; KI-Ausgaben und technische Nutzungsmetadaten, soweit erforderlich

- Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind für HOLZPLANER24 nicht vorgesehen und sollen nach den Nutzungsbedingungen nicht eingestellt werden.

3.5. Von der Verarbeitung betroffen sind:

- Kunden des Auftraggebers
- Interessenten und Personen, die Leistungen des Auftraggebers anfragen
- Inhaber, Mitarbeiter und sonstige berechtigte Zugangsinhaber des Auftraggebers
- Ansprechpartner bei Geschäftskunden sowie Nutzer des HOLZPLANER24-Anfrageformulars, soweit deren Daten dem Auftraggeber zugeordnet werden

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.8. Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer unverzüglich mit.

4.10. Die zentrale Speicherung der HOLZPLANER24-Produktivdaten erfolgt auf einem Serverstandort in Deutschland. Soweit Unterauftragnehmer personenbezogene Daten außerhalb der EU bzw. des EWR verarbeiten

oder von dort aus Zugriffsmöglichkeiten bestehen, erfolgt dies ausschließlich unter Einhaltung der Anforderungen des Kapitels V DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission oder geeigneter Garantien nach Art. 46 DSGVO, soweit erforderlich.

5. Technische und organisatorische Maßnahmen

5.1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen (technische und organisatorische Maßnahmen) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

5.2. Die Maßnahmen gemäß vorheriger Ziffer können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

5.3. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6. Die Verarbeitung im Homeoffice oder außerhalb eigener Geschäftsräume ist zulässig, sofern hierbei ein dem Schutzniveau dieses Vertrags entsprechendes Sicherheitsniveau gewährleistet wird. Insbesondere sind Endgeräte gegen unbefugten Zugriff zu schützen, durch individuelle Benutzerauthentifizierung abzusichern, mit aktuellen Sicherheitsupdates zu betreiben und so zu verwenden, dass Dritte keine Einsicht in personenbezogene Daten erhalten. Eine gemeinsame Nutzung administrativer Zugänge mit unbefugten Personen ist unzulässig.

5.7. Physische Datenträger des Auftraggebers sind nicht Bestandteil der regulären HOLZPLANER24-Leistung. Soweit ausnahmsweise physische Datenträger verarbeitet werden, sind sie eindeutig zuzuordnen, angemessen gegen unbefugten Zugriff zu sichern und nach Abschluss der Verarbeitung zurückzugeben oder nach Weisung des Auftraggebers sicher zu vernichten.

5.8. Der Auftraggeber ist berechtigt, die Erfüllung der Pflichten durch den Auftragnehmer, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihre Wirksamkeit, unter Vorankündigung mit angemessener Frist zu kontrollieren und zu überprüfen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu diesem Zweck und für die Dauer der Kontrolle Zugang zu allen relevanten Räumlichkeiten sowie Einsicht in und Zugriff auf alle für die Prüfung erforderlichen Dokumente und Systeme zu verschaffen.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

6.2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7. Unterauftragsverhältnisse

7.1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Beauftragung der in Anlage 2 aufgeführten Unterauftragnehmer. Der Auftragnehmer informiert den Auftraggeber rechtzeitig über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragnehmern, sodass der Auftraggeber Gelegenheit erhält, aus berechtigten datenschutzrechtlichen Gründen Einwände gegen die Änderung zu erheben. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers Auskunft über die

gegenwärtig und in der Vergangenheit für die Auftragsverarbeitung eingesetzten Unterauftragnehmer zu erteilen und die datenschutzrechtliche Einbindung nachzuweisen.

7.2. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.3. Weitere Subbeauftragungen durch den Subunternehmer sind nach den Maßgaben der Ziffer 7.1. zulässig.

7.4. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.5. Die Beauftragung von Subunternehmern im Sinne von Ziffer 7.1. und Ziffer 7.3., die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU, des EWR oder Staaten erbringen, für die ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO gilt, ist nur bei Beachtung der in Ziffer 4.10. dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

7.6. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig angemessen zu überprüfen und die Ergebnisse zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf dessen Verlangen hin vorzulegen.

7.7. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.8. Zurzeit sind die in Anlage 2 mit Namen und Anschrift bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang betraut. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

7.9. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

8.1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen im Sinne der Ziffer 5 sowie ihre Wirksamkeit, beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

8.5. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden

Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

8.6. Der Auftraggeber kann HOLZPLANER24 freiwillig mit eigenen Konten bei Drittanbietern verbinden, insbesondere mit Buchhaltungs-, Kontakt-, Kalender- oder vergleichbaren Diensten. Soweit der Auftragnehmer auf Veranlassung oder Weisung des Auftraggebers personenbezogene Daten an einen vom Auftraggeber ausgewählten Drittanbieter übermittelt oder von diesem abruft, erfolgt dies ausschließlich zur Ausführung der vom Auftraggeber aktivierten Schnittstelle.

8.7. Drittanbieter, die vom Auftraggeber selbst ausgewählt und auf Grundlage eines eigenen Vertragsverhältnisses des Auftraggebers genutzt werden, gelten nicht allein aufgrund der technischen Anbindung als Unterauftragnehmer des Auftragnehmers, soweit sie nicht vom Auftragnehmer selbst zur Erbringung der Hauptleistung beauftragt werden. Der Auftraggeber bleibt insbesondere für die Auswahl des Drittanbieters, die Zulässigkeit seiner Nutzung, die erforderlichen datenschutzrechtlichen Rechtsgrundlagen und Informationspflichten sowie - soweit erforderlich - den Abschluss eines Vertrags zur Auftragsverarbeitung mit dem Drittanbieter verantwortlich.

8.8. Der Auftragnehmer beschränkt den Datenaustausch über solche Schnittstellen auf den für die jeweils aktivierte Funktion erforderlichen Umfang und schützt Zugangsdaten, API-Tokens sowie technische Verknüpfungsinformationen nach dem Stand der Technik. Wird eine Schnittstelle getrennt, werden beim Auftragnehmer gespeicherte Zugangsdaten bzw. Tokens deaktiviert oder gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Bereits beim Drittanbieter gespeicherte Daten unterliegen dem Vertragsverhältnis zwischen dem Auftraggeber und dem jeweiligen Drittanbieter.

9. Mitteilungspflichten

9.1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

9.2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2. Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

10.3. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder zu einer Haftung des Auftragnehmers führen kann. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10.5. Zu einer materiell-rechtlichen Prüfung von Weisungen ist der Auftragnehmer nicht verpflichtet.

11. Beendigung des Auftrags

11.1. Bei Beendigung des Auftragsverhältnisses oder auf dokumentiertes Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers zurückzugeben bzw. zum Export bereitzustellen oder zu löschen, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Sofern keine unverzügliche Löschung angewiesen wird, wird nach Vertragsende für bis zu 30 Kalendertage ein maschinenlesbarer Export bereitgestellt. Nach Ablauf dieser Frist werden die Produktivdaten gelöscht. Restkopien in lokalen Sicherungsbeständen werden spätestens mit Ablauf des dokumentierten lokalen Aufbewahrungszyklus von 14 Tagen überschrieben bzw. gelöscht; Restkopien im Offsite-Backup spätestens mit Ablauf des dokumentierten Aufbewahrungszyklus von 30 täglichen Sicherungsständen. Bis dahin sind die Restkopien gesperrt und werden nicht produktiv genutzt. Elektronische Produktivdaten sind so zu löschen, dass eine Wiederherstellung mit vertretbarem Aufwand nicht mehr möglich ist. Soweit ausnahmsweise physische Datenträger zu vernichten sind, erfolgt dies nach einem dem Schutzbedarf angemessenen Verfahren.

11.2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber auf Verlangen vorzulegen.

11.4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13. Haftung

13.1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

13.2. Der Auftraggeber trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit personenbezogene Daten in seiner Verantwortung vom Auftragnehmer unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftraggeber dem Auftragnehmer ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

13.3. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

13.4. Die Ziffer 13.3 gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14. Sonderkündigungsrecht

14.1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

14.2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14.3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. Sonstiges

15.1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

15.2. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

15.3. Für Nebenabreden ist die Schriftform erforderlich.

15.4. Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

15.5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

_____	_____
Ort, Datum	Ort, Datum
Auftragnehmer	**Auftraggeber**

Anlage 1 - Technische und organisatorische Maßnahmen

Im Folgenden werden die für HOLZPLANER24 geltenden technischen und organisatorischen Maßnahmen beschrieben. Sie sind entsprechend dem Stand der Technik und dem jeweiligen Risiko fortlaufend zu überprüfen und bei Bedarf anzupassen, ohne das vereinbarte Schutzniveau zu unterschreiten.

1. Zutrittskontrolle

Produktivdaten werden auf einem virtuellen Server der netcup GmbH am Serverstandort Nürnberg, Deutschland, verarbeitet; ein eigener öffentlich zugänglicher Serverraum wird nicht betrieben. Administrative

Endgeräte befinden sich in nicht öffentlich zugänglichen, gegen unbefugten Zutritt geschützten Räumen. Die physische Rechenzentrumssicherheit obliegt dem in Anlage 2 genannten Infrastruktur-Unterauftragnehmer.

2. Zugangskontrolle

Zugänge zu HOLZPLANER24 sind benutzerbezogen. Die Authentifizierung und die PostgreSQL-basierte Anwendungsdatenbank werden selbst gehostet auf der HOLZPLANER24-Serverumgebung betrieben. Für neue Passwörter gilt anwendungsseitig eine Mindestlänge von 12 Zeichen; Passwörter werden ausschließlich als kryptografische Hashwerte gespeichert. Cloudflare Turnstile dient als Bot-/Missbrauchsschutz bei sicherheitsrelevanten Formularen. Administrations- und Service-Schlüssel werden ausschließlich serverseitig als geschützte Umgebungsvariablen bzw. Secret-Dateien verwendet und nicht im Frontend ausgeliefert. Administrationskonten bei Hosting-, Deployment- und Infrastruktur-Anbietern werden, soweit technisch angeboten, durch Mehrfaktor-Authentifizierung abgesichert; der Serverzugang erfolgt vorzugsweise über individuelle SSH-Schlüssel.

3. Zugriffskontrolle und Mandantentrennung

Daten werden mandantenbezogen getrennt. In der Datenbank werden Row-Level-Security-Regeln und Mandanten-/Betriebszuordnungen eingesetzt. Nutzer erhalten nur Zugriff auf die ihrem Betrieb zugeordneten Daten. HOLZPLANER24 wird in einer eigenen Container-/Docker-Umgebung mit eigener Datenbank, eigenen Volumes, Secrets und Netzwerksegmenten betrieben und logisch von anderen Anwendungen des Auftragnehmers getrennt. Administrative Produktfunktionen sind rollenbasiert beschränkt; routinemäßige Einsicht in Kundendateninhalte der Händler ist nicht vorgesehen.

4. Transport- und Weitergabekontrolle

Die Übertragung zwischen Browser, dem über Netlify ausgelieferten Frontend und der HOLZPLANER24-API auf dem Server der netcup GmbH erfolgt ausschließlich über TLS/HTTPS. Zugangsdaten und geheime Service-Schlüssel werden nicht unverschlüsselt an Clients ausgeliefert. Der öffentliche Serverzugriff wird auf die für den Betrieb erforderlichen Dienste beschränkt; administrative Zugänge werden durch Firewall-Regeln, SSH-Schlüssel und rollenbezogene Berechtigungen geschützt. Übermittlungen an Unterauftragnehmer erfolgen nur im für die Leistungserbringung erforderlichen Umfang.

5. Eingabe- und Nachvollziehbarkeitskontrolle

Änderungen in der Anwendung erfolgen grundsätzlich im Kontext authentifizierter Nutzer. Für wesentliche Geschäftsobjekte sind Zeitstempel, Statusinformationen und - soweit technisch vorgesehen - Aktivitäts-/Auditprotokolle vorhanden. Rechnungsnummern werden datenbankgestützt vergeben; festgeschriebene Rechnungsinhalte werden gegen unbeabsichtigtes Überschreiben geschützt.

6. Auftragskontrolle

Personenbezogene Daten werden nur zur Erbringung von HOLZPLANER24 und nach Weisung des Auftraggebers verarbeitet. Unterauftragnehmer werden vertraglich/datenschutzrechtlich eingebunden und in Anlage 2 dokumentiert. Produktionszugriffe werden auf das erforderliche Maß beschränkt.

7. Verfügbarkeit und Wiederherstellbarkeit

Die primäre HOLZPLANER24-Datenbank, die Authentifizierung und das Backend werden auf einem VPS der netcup GmbH am Standort Nürnberg, Deutschland, betrieben. Das statische Frontend wird über Netlify bereitgestellt. Für die Datenbank werden täglich automatisierte Sicherungen erstellt. Lokale Sicherungen werden 14 Tage vorgehalten. Zusätzlich werden Sicherungen in ein vom Produktivbetrieb logisch getrenntes, verschlüsseltes Offsite-Backup übertragen; dort werden 30 tägliche Sicherungsstände vorgehalten. Vor wesentlichen Systemänderungen können ergänzend Server-Snapshots erstellt werden; Snapshots ersetzen die Datenbanksicherung nicht. Die erfolgreiche Ausführung der Sicherungsjobs wird überwacht und mindestens vierteljährlich wird eine Wiederherstellung stichprobenartig getestet und dokumentiert. HOLZPLANER24 bietet einen vollständigen Datenexport in maschinenlesbaren Formaten (u. a. ZIP/CSV/JSON) an.

8. Trennungsgebot

Daten unterschiedlicher Auftraggeber werden logisch über Mandanten-/Betriebskennungen und Datenbankrichtlinien voneinander getrennt. Test- und Musterdaten werden nicht automatisch in neue Kundenkonten eingespielt.

9. Löschung, Rückgabe und Datenportabilität

Der Auftraggeber kann seine Daten über die Exportfunktion herausgeben lassen. Daten werden auf dokumentierte Weisung berichtigt oder gelöscht. Nach Vertragsende wird, sofern keine unverzügliche Löschung verlangt wird, für bis zu 30 Kalendertage ein maschinenlesbarer Export bereitgestellt. Anschließend werden die Produktivdaten gemäß Ziffer 11 gelöscht. In lokalen Sicherungsbeständen verbliebene Restkopien werden innerhalb des 14-tägigen Aufbewahrungszyklus überschrieben bzw. gelöscht. Restkopien im Offsite-Backup werden innerhalb des Aufbewahrungszyklus von 30 täglichen Sicherungsständen entfernt. Bis dahin sind sie gesperrt und werden nicht produktiv genutzt.

10. Vertraulichkeit und organisatorische Sicherheit

Zugriffsberechtigte Personen sind zur Vertraulichkeit verpflichtet. Betriebssysteme, Browser und Sicherheitssoftware auf administrativen Endgeräten sind aktuell zu halten. Geräte sind durch Benutzerauthentifizierung zu schützen; Datenträger mobiler Geräte sind nach Möglichkeit verschlüsselt.

11. Datenschutzfreundliche Voreinstellungen und Datenminimierung

HOLZPLANER24 ist auf B2B-Nutzung in Deutschland und - soweit vertraglich angeboten - in weiteren Staaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums ausgerichtet. Es werden keine besonderen Kategorien personenbezogener Daten benötigt. Werbe-/Marketing-Tracking ist derzeit nicht Bestandteil der Anwendung. Öffentliche Händlerprofile werden nur bei ausdrücklicher Freigabe des jeweiligen Betriebs veröffentlicht. Optionale Schnittstellen, insbesondere Buchhaltungs-, Kontakt- und Kalenderintegrationen, werden nur nach aktiver Verbindung durch den Auftraggeber genutzt und auf den für die jeweilige Funktion erforderlichen Datenumfang beschränkt. Zugangsdaten und API-Tokens für solche Verbindungen werden nicht im Klartext an Browser-Clients ausgeliefert und nur für die aktivierte Schnittstelle verwendet.

12. Vorfallmanagement

Datenschutz- und Sicherheitsvorfälle werden dokumentiert und nach Ziffer 9 dieses Vertrags unverzüglich, spätestens innerhalb der dort vereinbarten Frist, an den Auftraggeber gemeldet. Kontaktstelle des Auftragnehmers: kontakt@sz-digital-lab.de.

Anlage 2 - Gegenwärtige Unterauftragnehmer (Stand 17.10.2026)

Der Auftragnehmer bedient sich zur Erbringung der Datenverarbeitungen im Auftrag der folgenden Unterauftragnehmer:

Die nachfolgende Liste dokumentiert die zum Stand 17.10.2026 für die Auftragsverarbeitung vorgesehenen bzw. eingesetzten Unterauftragnehmer. Bei Änderungen informiert der Auftragnehmer bestehende Kunden entsprechend Ziffer 7.1 rechtzeitig und ermöglicht berechtigte datenschutzrechtliche Einwände. Diese Aktualisierung ersetzt eine etwa erforderliche Kundenbenachrichtigung oder vertragliche Zustimmung nicht.

Unterauftragnehmer	Anschrift	Leistung / Verarbeitungsumfang	Hinweis
netcup GmbH	Emmy-Noether-Straße 10 76131 Karlsruhe Deutschland	VPS-Infrastruktur für HOLZPLANER24: Backend, PostgreSQL-Datenbank, Authentifizierung, Container/Volumes und Backup-Speicher. Produktivserver am Standort Nürnberg, Deutschland.	Kernverarbeitung in Deutschland. Vertragliche Einbindung über einen AV-Vertrag gemäß Art. 28 DSGVO im netcup Customer Control Panel.
Netlify, Inc.	101 2nd Street San Francisco, CA 94105 USA	Hosting, Deployment und CDN-Auslieferung des HOLZPLANER24-Frontends; hierbei können technische Verbindungs- und Protokolldaten (z. B. IP-Adresse, Zeitpunkt, abgerufene Ressource) verarbeitet werden. Keine primäre Speicherung der HOLZPLANER24-Kundendatensätze.	Drittlandbezug möglich; Verarbeitung nach dem jeweils geltenden Netlify Data Processing Agreement und den dort vorgesehenen Transfermechanismen.
Cloudflare, Inc.	101 Townsend Street San Francisco, CA 94107 USA	Cloudflare Turnstile als Bot-/Missbrauchsschutz bei Registrierung, Login und ausgewählten öffentlichen Formularen; Verarbeitung insbesondere technischer Browser- und Verbindungsdaten.	Nur soweit Turnstile eingesetzt wird. Drittlandbezug möglich; Verarbeitung nach dem jeweils geltenden Cloudflare Data Processing Addendum und den anwendbaren Transfermechanismen.
Brevo GmbH	Köpenicker Straße 126 10179 Berlin Deutschland	Versand transaktionaler System-E-Mails für HOLZPLANER24 (z. B. Registrierung, Passwort-Zurücksetzung, Konto- und Servicehinweise); verarbeitet insbesondere Empfänger-E-Mail-Adresse und den jeweiligen Nachrichteninhalt.	Verarbeitung nach dem jeweils geltenden Brevo Data Processing Agreement. Maßgeblich ist die im Brevo-Konto bzw. auf der Abrechnung ausgewiesene Vertragsgesellschaft; bei der deutschen Gesellschaft: Brevo GmbH, Berlin.

Unterauftragnehmer	Anschrift	Leistung / Verarbeitungsumfang	Hinweis
OpenAI Ireland Ltd.	1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper Dublin 1, D01 YC43 Irland	Bereitstellung KI-gestützter HOLZPLANER24-Funktionen über eine serverseitig angebundene OpenAI-API: (1) Auswertung von nach aktiver Nutzeraktion übermittelten, zuvor extrahierten Belegtexten zur Erkennung von Lieferant, Datum, Positionen, Beträgen und Zuordnungsvorschlägen; (2) Beantwortung von Bedienungsfragen zur Software anhand der übermittelten Frage und des Themen-/Seitenkontexts. Belegtexte können personenbezogene Angaben enthalten. Die KI selbst schreibt keine Buchungen. Original-Belegdateien werden für die KI-Belegerkennung nicht an OpenAI übermittelt.	Einsatz als Unterauftragsverarbeiter für optionale KI-Aufrufe; OpenAI Data Processing Addendum (DPA, derzeit geltende Fassung) und dessen Subprozessorenliste beachten. Verarbeitung/Weiterübermittlung außerhalb EU/EWR möglich; Drittlandtransfers nur nach den geltenden Garantien des DPA (z. B. SCC/Angemessenheitsbeschluss). Keine Zusage ausschließlicher EU-Verarbeitung. Standardmäßig kein KI-Training mit API-Inhalten ohne Opt-in; bis zu 30 Tage Aufbewahrung für Missbrauchsüberwachung, vorbehaltlich der geltenden Ausnahmen. Bestehende Kunden vor Änderung gemäß Ziffer 7.1 informieren.

Anlage 3 - Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

1. Weisungserteilung

Auftraggeber: [Name, Funktion, E-Mail der weisungsberechtigten Person]

2. Weisungsentgegennahme

Auftragnehmer: Sascha Zeiser, SZ Digital Lab, kontakt@sz-digital-lab.de

Dokumentenstand: 17.10.2026 – Version AVV-2026-10-17-EU-3; Ergänzung von Zweck/Datenkategorien und Unterauftragnehmer OpenAI Ireland Ltd.

Diese Fassung aktualisiert die EU/EWR-Fassung vom 13.09.2026 hinsichtlich der optionalen KI-Verarbeitung und Anlage 2 (OpenAI Ireland Ltd.). Für bestehende Kundenverträge sind die Mitteilungs- und Einwandsregelungen aus Ziffer 7.1 zu beachten. Die vertragliche Aktualisierung ist nicht rückwirkend allein durch die Veröffentlichung abgeschlossen.