Bedingungen

Meisterplan Software as a Service Bedingungen

Zuletzt aktualisiert am 07.11.2023

Meisterplan Software as a Service Bedingungen (nachfolgend „**Bedingungen**" genannt) zu einer Vereinbarung (nachfolgend **„Vereinbarung"** genannt), die über den Meisterplan-Webshop oder auf eine andere Weise zwischen itdesign GmbH, Friedrichstr. 12, 72072 Tübingen (nachfolgend **„Anbieter"** genannt) und Ihnen bzw. der Firma/Organisation, die Sie vertreten (nachfolgend **„Kunde"** genannt) zustande kommt. Anbieter und Kunde werden nachfolgend zusammen **„Parteien"** genannt.

Diese Bedingungen setzen sich zusammen aus

- den nachfolgenden Regelungen für die Erbringung der Services durch den Anbieter (Teil I) (nachfolgend **„Servicevertrag"** genannt) sowie
- der Vereinbarung über die Auftragsverarbeitung zwischen den Parteien (Teil II) (nachfolgend **„Auftragsverarbeitungsvertrag"** genannt).

Teil I – Servicevertrag

§ 1 Gegenstand der Vereinbarung, Definitionen

(1) Mit der Vereinbarung vereinbaren die Parteien, dass der Anbieter dem Kunden die Nutzungsmöglichkeit für die Softwareanwendung „Meisterplan" (im Folgenden **„Anwendung"** genannt) zum Zugriff gegen Entgelt zur Verfügung stellt.

(2) Gegenstand der Vereinbarung ist die Bereitstellung der vom Anbieter aktuell zur Verfügung gestellten Version der Anwendung zur Nutzung ihrer Funktionalitäten, die technische Ermöglichung der Nutzung der Anwendung und die Einräumung bzw. Vermittlung von Nutzungsrechten an der Anwendung gegen Zahlung des in der Vereinbarung festgelegten Entgelts für den in der Vereinbarung oder in einer separaten Vereinbarung festgelegten Zeitraum.

(3) Eine Funktionsbeschreibung der Anwendung kann unter https://meisterplan.com/de/wp-content/uploads/pdfs/meisterplan-product-description.pdf abgerufen werden.

Die vom Anbieter zur Nutzung der Anwendung freigegebene Softwareumgebung, insbesondere Browser, sind in den Systemvoraussetzungen der Anwendung festgelegt und unter https://meisterplan.com/de/wp-content/uploads/pdfs/meisterplan-system-requirements.pdf abrufbar.

(4) Ressource: Eine „**Ressource**" ist im Folgenden eine natürliche Person oder materielle Ressource, die mit der Anwendung verwaltet werden kann. Jede Ressource kann sich zudem als Nutzer der Anwendung anmelden. Nutzt der Kunde „Platzhalter", „Proxy-Ressourcen" oder Rollen, so muss für jede dadurch dargestellte Person oder materielle Ressource eine Ressource lizenziert werden.

Umgebung: Eine „**Umgebung**" ist eine logische Einheit, auf der die Anwendung betrieben wird. Dies kann ein physischer oder ein virtueller Server sein, auf den mithilfe eines Browsers zugegriffen werden kann.

§ 2 Bereitstellung der Anwendung, Sicherung der Anwendungsdaten

(1) Der Anbieter hält auf einer zentralen Datenverarbeitungsanlage oder mehreren Datenverarbeitungsanlagen (auch bei Mehrzahl im Folgenden **„Server"** genannt) die Anwendung in der jeweils aktuellen Version nach Maßgabe der folgenden Regelungen bereit.

(2) Die Anwendung und die vom Kunden in selbige Anwendung eingegebenen Daten (im Folgenden **„Anwendungsdaten"** genannt) werden auf dem Server regelmäßig, sofern nicht anders zwischen den Parteien vereinbart mindestens kalendertäglich gesichert. Das durch diese Datensicherung entstehende Backup wird auf dem Server abgelegt. Die so abgelegte Datensicherung wird dreißig (30) Kalendertage geführt und am darauffolgenden Arbeitstag durch automatische Prozesse überschrieben.

(3) Übergabepunkt für die Anwendung und die Anwendungsdaten ist der Routerausgang des vom Anbieter genutzten Rechenzentrums (im Folgenden **„Übergabepunkt"** genannt).

(4) Wenn Sie ein Wettbewerber sind ist es Ihnen ausdrücklich untersagt, die Anwendung zu nutzen oder darauf zuzugreifen. Unter einem Wettbewerber verstehen wir eine Einzelperson oder eine Einheit, die in einem Geschäftsfeld tätig ist, das Produkte oder Dienstleistungen anbietet, die denen von Meisterplan ähnlich sind, einschließlich Mitarbeitern, freien Mitarbeitern oder sonstigen Vertretern oder Beauftragten, Dieses Verbot erstreckt sich auch auf die Anmeldung für kostenlose Testversionen. Darüber hinaus dürfen Sie die Anwendung nicht nutzen, um ihre Verfügbarkeit, Performance oder sonstige Funktionalität zu überwachen oder für jegliche anderen Benchmarking- oder Wettbewerbszwecke zu verwenden.

§ 3 Software-Testversionen

Der Kunde hat die Möglichkeit, die Anwendung kostenlos zu testen. Die kostenlose Software-Testversion der Anwendung wird dem Kunden ausschließlich für Testzwecke für einen begrenzten Zeitraum durch den Lizenzgeber überlassen. Eine Testversion dient nicht dem Einsatz im laufenden Geschäftsbetrieb.

30 Tage nach Ende der Testphase werden die Anwendungsdaten automatisch gelöscht.

§ 4 Service Levels

In diesem Paragraphen werden die generellen Service Levels für die Nutzung der Anwendung festgelegt.

(1) Technische Verfügbarkeit der Anwendung

a) Der Anbieter stellt dem Kunden die Anwendung während der Systemlaufzeit bereit, dies aber unter Ausschluss der vereinbarten Zeiten geplanter Nichtverfügbarkeit nach nachfolgendem § 4 (2).

Die **„Systemlaufzeit"** beläuft sich auf 24 Stunden am Tag und 365 Tage im Jahr.

b) Die Zeiten der verfügbaren Nutzung (das heißt die Verfügbarkeit ist gegeben) vereinbaren die Parteien wie folgt: Innerhalb der Systemlaufzeit wird eine Hauptnutzungszeit definiert, während derer der Anbieter die monatliche Verfügbarkeit der Anwendung von Montag bis Freitag von 09.00 – 17.00 ME(S)Z zu 99% sichergestellt. Innerhalb dieser Zeit wird die längste ununterbrochene Ausfallzeit 4 Stunden nicht überschreiten.

Alle Zeiten außerhalb der Hauptnutzungszeit gelten als Nebennutzungszeit, in der die Verfügbarkeit nicht gewährleistet wird. Darunter fallen Samstage, Sonntage sowie der 1. Januar und 25. Dezember.

c) Zur verfügbaren Nutzung zählen auch die Zeiträume, während denen

- Störungen vorliegen, die ihre Ursache im lokalen IT-System des Kunden oder in einer Störung der Anbindung des Kunden an den Übergabepunkt haben oder
- sonstige Ereignisse eintreten, die nicht vom Anbieter oder einer seiner Erfüllungsgehilfen verursacht wurden, z. B. durch höhere Gewalt, Missbrauch oder Bedienfehler.

(2) Geplante Nichtverfügbarkeit

Der Anbieter ist in Zeiten außerhalb der Hauptnutzungszeit berechtigt, die Anwendung und/oder Server zu warten, zu pflegen sowie sonstige Arbeiten vorzunehmen. Geplante Nichtverfügbarkeiten wird der Anbieter dem Kunden 7 Tage im Voraus unter https://status.meisterplan.com ankündigen.

Wenn und soweit der Kunde in Zeiten der geplanten Nichtverfügbarkeit die Anwendung nutzen kann, so besteht hierauf kein Rechtsanspruch. Kommt es bei einer Nutzung der Anwendung in Zeiten der geplanten Nichtverfügbarkeit zu einer Leistungsreduzierung oder Leistungseinstellung, besteht für den Kunden kein Anspruch auf Mangelhaftung oder Schadenersatz.

(3) Messung der tatsächlichen Verfügbarkeit

Die tatsächliche Verfügbarkeit in Prozent berechnet sich für die Hauptnutzungszeit wie folgt:

$$\frac{Zeit\ der\ tatsächlichen\ Verfügbarkeit\ in\ der\ Hauptnutzungszeit\ in\ Sekunden}{Zeitraum\ der\ Hauptnutzungszeit\ im\ jeweiligen\ Monat\ in\ Sekunden} * 100$$

Die Verfügbarkeit wird durch eine vom Anbieter geführte Überwachungsinstanz festgehalten. Dabei werden die Verfügbarkeit der Anwendung an sich sowie der Anwendungs-Dienste (wie etwa Reporting) überwacht.

Auf der Grundlage dieser Überwachungsinstanz werden maschinell Daten über die Verfügbarkeit erzeugt, die der Anbieter dem Kunden unter https://status.meisterplan.com zur Verfügung stellt.

(4) Reaktionszeiten

Der Anbieter trägt nur innerhalb der Hauptnutzungszeit dafür Sorge, dass innerhalb einer von der jeweiligen, nachfolgend definierten Störungsklasse abhängigen, nachfolgend vereinbarten Zeit ab Zugang einer Meldung einer technischen Störung des Kunden per E-Mail oder Support-Ticket mit den Störungsbehebungsarbeiten begonnen wird (**„Reaktionszeit"**).

Bei außerhalb der Hauptnutzungszeit gemeldeten Störungen beginnt die Reaktionszeit mit dem nächsten Werktag innerhalb der Hauptnutzungszeit.

Störungsklasse Reaktionszeit
Störungsklasse 1 4 Stunden
Störungsklasse 2 2 Werktage
Störungsklasse 3 5 Werktage

Die Störungsklassen werden dabei wie folgt definiert:

Klasse 1: Betriebsverhindernder Mangel: Ein betriebsverhindernder Mangel liegt vor, wenn die Nutzung der Anwendung unmöglich ist; eine Umgehungslösung existiert nicht.

Klasse 2: Betriebsbehindernder Mangel: Ein betriebsbehindernder Mangel liegt vor, wenn die Nutzung der Anwendung eingeschränkt ist, ohne dass eine Umgehungslösung zur Verfügung steht.

Klasse 3: Leichter Mangel: Ein leichter Mangel liegt vor, wenn die Nutzung der Anwendung ohne oder mit unwesentlichen Einschränkungen möglich ist.

(5) Verstoß gegen die Verfügbarkeiten und Abhilfe

Verstößt der Anbieter gegen die unter § 4 (1) festgelegten Verfügbarkeiten während der Hauptnutzungszeit, ist der Kunde berechtigt, eine Vertragsstrafe (im Folgenden **„Service Level Credit"** genannt) in folgendem Umfang zu verlangen:

- Bei einer Unterschreitung der Verfügbarkeit in der Hauptnutzungszeit: 0,5% der monatlichen Vergütung (pro rata) pro angefangenen 0,1% Unterschreitung der vereinbarten Verfügbarkeit, maximal jedoch 100% der monatlichen Vergütung;
- Bei einer Überschreitung der längsten ununterbrochenen Ausfallzeit in der Hauptnutzungszeit: 5% der monatlichen Vergütung (pro rata) pro Überschreitungsfall, maximal jedoch 100% der monatlichen Vergütung;
- Bei einer Überschreitung der Reaktionszeit in der Hauptnutzungszeit bei Vorliegen eines Mangels der Störungsklasse 1: 5% der monatlichen Vergütung (pro rata) pro Überschreitungsfall, maximal jedoch 100% der monatlichen Vergütung.

Dies gilt nicht, soweit der Anbieter die Unterschreitung der Verfügbarkeit/Überschreitung der Ausfallzeit/Reaktionszeit nicht zu vertreten hat.

Der Wert der insgesamt verwirkten Service Level Credits wird an den Kunden ausbezahlt oder mit laufenden Rechnungen des Anbieters verrechnet.

Die Service Level Credits werden auf etwaige Schadensersatzansprüche des Kunden angerechnet. Der Kunde kann unabhängig von der Geltendmachung von Service Level Credits die Weitererfüllung der Vereinbarung durch den Anbieter verlangen.

§ 5 Sonstige Leistungen des Anbieters, Online-Handbuch

(1) Der Anbieter wird dem Kunden während der Laufzeit der Vereinbarung entwickelte Neufassungen der Anwendung zur Verfügung stellen. Die neuen Fassungen können auch Funktionserweiterungen beinhalten.

Ein Anspruch des Kunden zur Erstellung von neuen Fassungen oder auf die Aufnahme bestimmter zusätzlicher Funktionalitäten in die Anwendung besteht nicht.

(2) Der Anbieter stellt dem Kunden über die Anwendung ein Online-Handbuch zur Verfügung.

§ 6 Nutzungsrechte, Rechte des Anbieters bei Überschreitung der Nutzungsbefugnisse

(1) Der Kunde erhält an der Anwendung ein einfaches, nicht ausschließliches, nicht unterlizenzierbares und nicht übertragbares, auf die Laufzeit der Vereinbarung befristetes Nutzungsrecht nach Maßgabe dieser Bedingungen.

Der Kunde darf die Anwendung nur für seine eigenen geschäftlichen Tätigkeiten durch eigenes Personal, Personal verbundener Gesellschaften, freie Mitarbeiter oder Handelsvertreter nutzen.

(2) Der Kunde darf die Anwendung nur durch die in der Vereinbarung vereinbarte Anzahl von Ressourcen im Sinne des § 1 (4) nutzen.

(3) Der Kunde erhält Zugang zu einer (1) Umgebung. Es werden keine zusätzlichen Umgebungen für Test- oder Qualitätssicherungszwecke bereitgestellt. Diese können bei Bedarf gegen getrennte Bezahlung hinzugebucht werden.

(4) Rechte, die vorstehend nicht ausdrücklich dem Kunden eingeräumt werden, stehen dem Kunden nicht zu. Der Kunde ist insbesondere nicht berechtigt, die Anwendung über die vereinbarte Nutzung hinaus zu nutzen oder von Dritten nutzen zu lassen oder die Anwendung Dritten zugänglich zu machen.

(5) Verletzt der Kunde die Verpflichtungen aus dem vorbenannten § 6 (1) bis (4) dieses Servicevertrags aus von ihm zu vertretenden Gründen, kann der Anbieter den Zugriff des Kunden auf die Anwendung oder die Anwendungsdaten sperren, wenn die Verletzung hierdurch nachweislich abgestellt werden kann.

Verletzt der Kunde trotz entsprechender schriftlicher Abmahnung des Anbieters weiterhin oder wiederholt die Verpflichtungen aus dem vorbenannten § 6 (1) bis (4) dieses Servicevertrags und hat er dies zu vertreten, so kann der Anbieter die Vereinbarung ohne Einhaltung einer Kündigungsfrist außerordentlich kündigen.

§ 7 Vergütung und Zahlung

(1) Für die zu erbringenden Leistungen der Nutzungsgewährung bezüglich der Anwendung bezahlt der Kunde an den Anbieter die sich aus der Vereinbarung ergebende Nutzungsvergütung zu den vereinbarten Zeitpunkten, zuzüglich jeweiliger gesetzlicher Mehrwertsteuer.

(2) Die Vergütung ist zu den in der Vereinbarung vereinbarten Zeitpunkten jeweils im Voraus zur Zahlung fällig.

(3) Der Anbieter ist berechtigt, die vereinbarten Preise für die vertraglichen Leistungen zum Ausgleich von Personalkosten und sonstigen Kostensteigerungen angemessen zu erhöhen. Der Anbieter wird dem Kunden eine Preiserhöhung schriftlich oder per E-Mail mitteilen; die Preiserhöhung gilt nicht für den Zeitraum, für den der Kunde bereits Zahlungen geleistet hat.

Eine Erhöhung der Preise innerhalb von 12 Monaten nach Abschluss der Vereinbarung ist ausgeschlossen.

(4) Im Fall einer vergütungspflichtigen Vereinbarung (also ausgenommen Test-Versionen) gewährt der Kunde dem Anbieter hiermit das Recht, das Firmenlogo des Kunden in Marketing-Materialien wie beispielsweise der Website des Anbieters zu verwenden, um den Kunden als einen Meisterplan-Kunden zu identifizieren. Dieser Nutzungsgenehmigung kann formlos per E-Mail an mail@meisterplan.com widersprochen werden. Davon abgesehen darf der Anbieter das Logo des Kunden nicht ohne vorherige schriftliche Erlaubnis verwenden.

§ 8 Mitwirkungspflichten des Kunden

(1) Der Kunde wird alle Pflichten und Obliegenheiten erfüllen, die zur Abwicklung der Vereinbarung erforderlich sind.

Der Kunde verpflichtet sich insbesondere,

1. die ihm bzw. den Nutzern zugeordneten Zugangsberechtigungen geheim zu halten, vor dem Zugriff durch Dritte zu schützen und nicht an unberechtigte Nutzer weiterzugeben.
2. die Nutzerkennung, Kennwörter und ähnliches durch geeignete und übliche Maßnahmen zu schützen; der Kunde wird den Anbieter unverzüglich unterrichten, wenn der Verdacht besteht, dass die Zugangsdaten und/oder Kennwörter nicht berechtigten Personen bekannt geworden sein könnten.
3. die Beschränkungen/Verpflichtungen im Hinblick auf die Nutzungsrechte nach § 6 dieses Servicevertrags einzuhalten, insbesondere
    - keine Informationen oder Daten unbefugt abzurufen oder abrufen zu lassen oder in Programme, die von dem Anbieter betrieben werden einzugreifen oder eingreifen zu lassen oder in Datennetze des Anbieters unbefugt einzudringen oder ein solches Eindringen zu fördern;

- den Anbieter von Ansprüchen Dritter freizustellen, die auf einer rechtswidrigen Verwendung der Anwendung durch den Kunden beruhen oder die sich aus vom Kunden verursachten datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung der Anwendung verbunden sind;
- die berechtigten Nutzer zu verpflichten, ihrerseits die für sie geltenden Bestimmungen der Vereinbarung und dieser Bedingungen einzuhalten;
- die berechtigten Nutzer nach Maßgabe der Art. 13 und 14 DSGVO über die Verarbeitung ihrer personenbezogenen Daten durch den Anbieter zu informieren.

4. vor der Versendung von Daten und Informationen an den Anbieter diese auf Viren zu prüfen und dem Stand der Technik entsprechende Virenschutzprogramme einzusetzen;
5. Mängel an Vertragsleistungen, insbesondere Mängel an den Leistungen nach § 1 dieses Servicevertrags, dem Anbieter unverzüglich anzuzeigen.

§ 9 Datensicherheit, Datenschutz

(1) Die Parteien werden die jeweils anwendbaren, insbesondere die in Deutschland gültigen datenschutzrechtlichen Bestimmungen beachten, wozu auch die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) zählt.

(2) Erhebt, verarbeitet oder nutzt der Kunde personenbezogene Daten, so steht er dafür ein, dass er dazu nach den anwendbaren, insbesondere datenschutzrechtlichen Bestimmungen berechtigt ist und stellt im Falle eines Verstoßes den Anbieter von Ansprüchen Dritter frei.

(3) Im Rahmen der Durchführung dieser Vereinbarung ist zwischen folgenden Kategorien von Daten zu unterscheiden, die z.T. personenbezogene Daten beinhalten können:

1. Der Anbieter verarbeitet personenbezogene Daten der Ansprechpartner beim Kunden (Kontaktperson, Adresse, Telefonnummer, Fax, E-Mail-Adresse), zur Vertragsdurchführung, insbesondere im Rahmen der Lizenzabrechnung. Diese Daten werden auf Basis berechtigter Interessen nach Art. 6 Abs. 1 Buchst. b) DSGVO verarbeitet. Zweck der Verarbeitung ist die Durchführung der Vereinbarung mit dem Kunden. Hinweise auf die Betroffenenrechte und Löschfristen ergeben sich aus den Datenschutzhinweisen des Anbieters, die unter https://meisterplan.com/de/datenschutz/ eingesehen werden können.
2. Der Anbieter verarbeitet Daten über das Nutzungsverhalten der Nutzer des Kunden im Rahmen von Server-Protokollen, die Information wie beispielsweise IP-Adresse, Zeitstempel oder Web-Anfrage enthalten können. Diese Daten werden auf Basis berechtigter Interessen nach Art. 6 Abs. 1 Buchst. f) DSGVO verarbeitet. Zweck ist zum einen die Suche und Behebung von Fehlern, die Abwehr von Gefahren und die Aufrechterhaltung des technischen Betriebs der Anwendung. Hinweise auf die Betroffenenrechte und Löschfristen ergeben sich aus den Datenschutzhinweisen des Anbieters, die unter https://meisterplan.com/de/datenschutz/ eingesehen werden können.

3. Der Anbieter verarbeitet statistische Daten zur Nutzung der Anwendung. Diese Daten enthalten keinerlei Inhalte, die Nutzer in der Anwendung eingegeben haben. Die Daten können die vom Nutzer ausgelöste Aktion, einen Zeitstempel, Informationen zum verwendeten Webbrowser, die interne ID der jeweiligen Datenbank, eine ID der Session, eine nicht-invertierbare Nutzerkennung, oder auch die ID eines auf der Website erzeugten Cookies enthalten. Diese Daten werden auf Basis berechtigter Interessen nach Art. 6 Abs. 1 Buchst. f) DSGVO verarbeitet. Zweck der Verarbeitung ist die dauerhafte Bereitstellung des Angebots, die Anpassung an sich entwickelnde Bedürfnisse der Nutzer, die Verbesserung der Nutzerfahrung in der Anwendung und die Optimierung der internen Prozesse des Anbieters. Hinweise auf die Betroffenenrechte und Löschfristen ergeben sich aus den Datenschutzhinweisen des Anbieters, die unter https://meisterplan.com/de/datenschutz/ eingesehen werden können.

4. Der Anbieter verarbeitet schließlich Anwendungsdaten, also diejenigen Daten, die der Kunde im Rahmen der Nutzung der Anwendung eingibt. Die Verarbeitung dieser Daten erfolgt im Auftrag des Kunden nach Maßgabe des Art. 28 DSGVO unter dem Auftragsverarbeitungsvertrag (Teil II dieser Bedingungen).

(4) Die Verpflichtungen nach § 9 (1) bis (3) bestehen, solange personenbezogene Daten im Einflussbereich des Anbieters liegen, auch über die Beendigung der Vereinbarung hinaus.

(5) Der Anbieter ist berechtigt, zur Erbringung seiner Leistungen Unterauftragnehmer einzusetzen. Eine fortlaufend aktualisierte Liste der jeweils vom Anbieter eingesetzten Unterauftragnehmer, die für ihn personenbezogene Daten verarbeiten, ist unter https://meisterplan.com/de/unterauftragnehmer/ einsehbar. Soweit der Anbieter Unterauftragnehmer mit der Verarbeitung personenbezogener Daten des Kunden betraut, die der Anbieter als Auftragsverarbeiter gemäß Art. 28 DSGVO verarbeitet, gelten die Sonderregelungen des Auftragsverarbeitungsvertrages (Teil II dieser Bedingungen). Solche Subunternehmer werden in einer separaten Liste aufgeführt.

(6) Der Kunde ist für die Inhalte, die im Rahmen der Nutzung der Anwendung eingegeben werden, verantwortlich und wird regelmäßig eigene Sicherungskopien erstellen, um bei Verlust von Daten und Informationen die Rekonstruktion derselben zu ermöglichen.

(7) Der Kunde wird, sofern und soweit ihm die technische Möglichkeit hierzu seitens des Anbieters eröffnet wird, regelmäßig die auf dem Server gespeicherten Anwendungsdaten durch Downloads sichern.

§ 10 Ansprüche bei Schlechtleistung

Im Fall der Schlechtleistung stehen dem Kunden die Ansprüche nach § 4 dieses Servicevertrages (Service Levels) zu. Im Übrigen gelten die gesetzlichen Bestimmungen.

§ 11 Vertraulichkeit

(1) Die Parteien verpflichten sich wechselseitig, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und sonstigen vertraulichen Informationen der jeweils anderen Partei vertraulich zu behandeln und ausschließlich für die Zwecke der Durchführung der Vereinbarung zu verwenden.

(2) Diese Verpflichtung bleibt auch nach Beendigung der Vereinbarung bestehen.

§ 12 Haftung

Die Haftung des Anbieters richtet sich nach dem Gesetz.

§ 13 Schutzrechte Dritter

(1) Der Anbieter steht dafür ein, dass die Anwendung frei von gewerblichen Schutzrechten und Urheberrechten Dritter ist.

Sofern ein Dritter wegen der Verletzung von Schutzrechten durch die Anwendung des Anbieters gegen den Kunden berechtigte Ansprüche erhebt, haftet der Anbieter gegenüber dem Kunden wie folgt:

1. Der Anbieter wird nach seiner Wahl und auf seine Kosten für die Anwendung oder den betreffenden Teil der Anwendung entweder ein Nutzungsrecht erwirken oder die Anwendung so ändern, dass das Schutzrecht nicht verletzt wird oder die Anwendung austauschen. Ist dies dem Anbieter nicht zu angemessenen Bedingungen möglich, stehen dem Kunden die gesetzlichen Rücktritts- oder Minderungsrechte zu.

2. Im Falle der rechtmäßigen Inanspruchnahme des Kunden durch einen Dritten stellt der Anbieter den Kunden von den Kosten, die durch die Geltendmachung dieser Ansprüche Dritter entstanden sind (darin eingeschlossen angemessene Rechtsanwaltskosten, beschränkt -sofern anwendbar- nach dem Rechtsanwaltsvergütungsgesetz), frei.

3. Die Pflicht des Anbieters zur Leistung von Schadenersatz richtet sich nach §12 dieses Servicevertrags.

Der Kunde verpflichtet sich, den Anbieter über die von Dritten geltend gemachten Ansprüche unverzüglich schriftlich oder per E-Mail zu verständigen; dem Anbieter sind alle Abwehrmaßnahmen und Vergleichsverhandlungen vorbehalten. Stellt der Kunde die Nutzung der Anwendung aus Schadensminderungs- oder sonstigen wichtigen Gründen ein, ist er verpflichtet, den Dritten darauf hinzuweisen, dass mit der Nutzungseinstellung kein Anerkenntnis einer Schutzrechtsverletzung verbunden ist.

(2) Ansprüche gegen den Anbieter nach § 13 (1) dieses Servicevertrags sind ausgeschlossen, wenn

1. der Kunde die Schutzrechtsverletzung zu vertreten hat,

2. die Behauptung einer Verletzung aus der unbefugten Modifikation der Anwendung entsteht oder mit einer solchen in Verbindung steht,

3. die Anwendung nicht gemäß den Regelungen der Vereinbarung und dieser Bedingungen oder in Übereinstimmung mit der Dokumentation der Anwendung genutzt wird,

4. die angebliche Verletzung durch die Nutzung eines von dem Anbieter herausgegebenen Updates, Upgrades oder Patch hätte verhindert werden können,
5. die angebliche Verletzung aus der Nutzung der Anwendung mit einem nicht vom Anbieter zur Verfügung gestellten Produkt eines Drittanbieters resultiert.

(3) Weitergehende Ansprüche des Kunden gegen den Anbieter und dessen Erfüllungsgehilfen wegen Ansprüchen aus der Verletzung von Schutzrechten Dritter sind ausgeschlossen.

§ 14 Abschluss der Vereinbarung, Start der Vereinbarung, Zeitraum, Kündigung

(1) Der Kunde gibt durch Klicken des Buttons „Kostenpflichtig Bestellen“ im Meisterplan-Webshop oder über andere Kommunikationswege eine Bestellung auf.

Die Vereinbarung wird abgeschlossen und das Vertragsverhältnis beginnt mit der Annahme der Bestellung des Kunden durch Auftragsbestätigung des Anbieters.

(2) Die Vereinbarung hat eine Mindestlaufzeit wie in der Vereinbarung festgelegt und ist bis zu diesem Zeitpunkt nicht ordentlich kündbar.

Die Vereinbarung verlängert sich jeweils um weitere Zeiträume der ursprünglich festgelegten Laufzeit, wenn sie nicht zum Ende der Mindestlaufzeit oder des jeweiligen Verlängerungszeitraumes von einer der Parteien gekündigt wird. Eine davon abweichende Kündigungsfrist kann von den Parteien schriftlich vereinbart werden.

(3) Das Recht zur Kündigung aus wichtigem Grund bleibt für die Parteien unberührt.

§ 15 Pflichten bei und nach Beendigung der Vereinbarung

Mit Beendigung des Vertragsverhältnisses erlöschen alle Rechte des Kunden zur Nutzung der Anwendung. Der Anbieter wird die Anwendungsdaten des Kunden 30 Tage nach Beendigung des Vertragsverhältnisses löschen.

§ 16 Höhere Gewalt, Leistungsverzögerungen

Leistungsverzögerungen aufgrund höherer Gewalt, hierzu zählen auch Ereignisse, die dem Anbieter die Leistungen nach der Vereinbarung wesentlich erschweren oder unmöglich machen, wie insbesondere Streik, Aussperrung, behördliche Anordnungen, der Ausfall von oder Störungen im Bereich von Kommunikationsnetzen und Gateways anderer Betreiber, soweit der Anbieter diese Ereignisse nicht verschuldet hat, hat der Anbieter nicht zu vertreten.

Der Anbieter ist berechtigt, die Leistungen um die Dauer der Behinderung hinauszuschieben oder zu unterbrechen.

§ 17 Schlussbestimmungen, Gerichtsstand, anwendbares Recht

(1) Alle Vereinbarungen, Nebenabreden und Zusicherungen sowie nachträgliche Änderungen und Ergänzungen der Vereinbarung und/oder dieser Bedingungen bedürfen einer entsprechenden Einigung zwischen den Parteien.

(2) Sollte eine Bestimmung der Vereinbarung und/oder dieser Bedingungen unwirksam sein oder werden oder sollten diese unvollständig sein, wird die Vereinbarung im Übrigen nicht berührt; es bleiben die übrigen Bestimmungen in Kraft.

Die Parteien werden sich in einem solchen Falle und im Falle vom Lücken, die die Parteien nicht vorhergesehen haben, auf eine Regelung einigen, die dem Sinn und Zweck der Vereinbarung und dieser Bedingungen am besten entspricht und die der unwirksamen Bestimmung am nächsten kommt.

(3) Die Vereinbarung und diese Bedingungen unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(4) Erfüllungsort und ausschließlicher Gerichtsstand für sämtliche aus oder im Zusammenhang mit der Vereinbarung und/oder dieser Bedingungen sich ergebenden Streitigkeiten ist Tübingen, Bundesrepublik Deutschland.

Teil II – Auftragsverarbeitungsvertrag

§ 1 Anwendungsbereich

(1) Die Parteien vereinbaren, dass der Anbieter bei Erbringung der Services als Auftragsverarbeiter für den Kunden tätig wird, soweit der Anbieter für den Kunden Anwendungsdaten verarbeitet (vgl. dazu die Definition der Anwendungsdaten in § 2(2) des Servicevertrages (Teil I dieser Bedingungen).

(2) Es wird darauf hingewiesen, dass der Anbieter personenbezogene Daten des Kunden verarbeiten kann, die nicht Gegenstand des Auftragsverhältnisses sind, da der Anbieter insoweit als Verantwortlicher agiert. Dies betrifft beispielsweise Daten zur Abrechnung und Lizenzverwaltung oder automatisch erhobene statistische Daten. Wegen der Einzelheiten wird auf die Regelungen des § 9 (3) des Servicevertrages (Teil I dieser Bedingungen) verwiesen. Es ist sichergestellt, dass diese Daten getrennt von den zur Verarbeitung überlassenen Anwendungsdaten gehalten werden. Ergänzend wird auf die Datenschutzhinweise des Anbieters verwiesen.

§ 2 Gegenstand des Auftrags

Der Anbieter verarbeitet auf Grundlage dieses Auftragsverarbeitungsvertrages personenbezogene Daten für den Kunden im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

§ 3 Dauer des Auftrags

(1) Die Laufzeit dieses Auftrags entspricht der Laufzeit der Vereinbarung.

(2) Der Kunde kann die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Anbieters gegen diesen Auftragsverarbeitungsvertrag vorliegt, der Anbieter eine Weisung des Kunden nicht ausführen kann oder will oder der Anbieter Kontrollrechte des Kunden vertragswidrig verweigert.

§ 4 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

(1) Gegenstand des Auftragsverhältnisses sind personenbezogene Anwendungsdaten, die der Kunde in die Anwendung eingibt, um sie dort verwalten zu können.

(2) Die Art der verarbeiteten personenbezogenen Daten bestimmt grundsätzlich der Kunde. Meisterplan bietet im Standard die Erfassung von Vorname, Nachname, E-Mail-Adresse, Rolle, Beschäftigungsbeginn- und Ende, PLZ und Stadt (keine persönliche Anschrift), Fähigkeiten (Skills) sowie die Verplanung auf Projekte. Der Kunde verpflichtet sich, keine besonderen Kategorien personenbezogener Daten in die Anwendung einzugeben.

(3) Typischerweise sind Betroffene Personen interne Mitarbeiter, externe Mitarbeiter und Zulieferer des Kunden. Der Kunde bestimmt über die Dateneingabe die Kategorien betroffener Personen; es können grundsätzlich Daten aller Kategorien betroffener Personen verarbeitet werden.

§ 5 Rechte und Pflichten sowie Weisungsbefugnisse des Kunden

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Kunde verantwortlich. Gleichwohl ist der Anbieter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Kunden gerichtet sind, unverzüglich an diesen weiterzuleiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen dem Kunden und dem Anbieter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(2) Der Kunde erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Der Kunde ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei dem Anbieter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(4) Der Kunde informiert den Anbieter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 6 Pflichten des Anbieters

(1) Der Anbieter verarbeitet die zur Verarbeitung überlassenen personenbezogenen Anwendungsdaten des Kunden ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern der Anbieter nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der

Anbieter als Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Anbieter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Der Anbieter verwendet die zur Verarbeitung überlassenen personenbezogenen Anwendungsdaten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate dieser Anwendungsdaten werden ohne Wissen des Kunden nicht erstellt.

(3) Der Anbieter sichert zu, dass die für den Kunden verarbeiteten Anwendungsdaten von sonstigen Datenbeständen strikt getrennt werden.

(4) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Kunden, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Kunden hat der Anbieter im notwendigen Umfang mitzuwirken und den Kunden soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

(5) Der Anbieter wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung nach Ansicht des Anbieters gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Anbieter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden nach Überprüfung bestätigt oder geändert wird.

(6) Der Anbieter hat personenbezogene Anwendungsdaten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Kunde dies mittels einer Weisung verlangt und berechtigte Interessen des Anbieters dem nicht entgegenstehen.

(7) Auskünfte über personenbezogene Anwendungsdaten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Anbieter nur nach vorheriger Weisung oder Zustimmung durch den Kunden erteilen.

(8) Der Anbieter erklärt sich damit einverstanden, dass der Kunde – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Kunden beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Anwendungsdaten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

(9) Der Anbieter sichert zu, dass der Anbieter, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(10) Der Anbieter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Anwendungsdaten des Kunden die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung der Vereinbarung fort.

(11) Der Anbieter sichert zu, dass der Anbieter die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht

und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO).

(12) Der Anbieter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(13) Der jeweils aktuell bestellte Beauftragte für den Datenschutz ist einsehbar unter https://meisterplan.com/de/datenschutz/

§ 7 Mitteilungspflichten des Anbieters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Anbieter teilt dem Kunden unverzüglich Störungen, Verstöße des Anbieters oder der bei ihr beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Anwendungsdaten mit.

(2) Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Kunden nach Art. 33 und Art. 34 DSGVO. Der Anbieter sichert zu, den Kunden erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(3) Meldungen nach Art. 33 oder 34 DSGVO für den Kunden darf der Anbieter nur nach vorheriger Weisung durchführen.

§ 8 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Anwendungsdaten des Kunden ist dem Anbieter nur mit Genehmigung des Kunden gestattet (Art. 28 Abs. 2 DSGVO). Der Anbieter hat dafür Sorge zu tragen, dass sie den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

(2) Je nachdem, von welchem Standort aus der Kunde die Registrierung vornimmt, entscheidet der Anbieter über den Rechenzentrumsstandort. Anwendungsdaten der Kunden, deren IP-Adresse auf einen EU-Standort schließen lässt, werden an einem Standort innerhalb der EU bzw. des EWR gehostet. Für alle anderen Standorte behält sich der Anbieter vor, über den Rechenzentrumsstandort frei zu bestimmen, einschließlich des Rechts zu einer Verarbeitung in den USA oder sonstigen Drittstaaten.

Eine Beauftragung von Subunternehmern oder sonstige Verarbeitung personenbezogener Daten des Kunden in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Der Anbieter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen dem Kunden und dem Anbieter insoweit auch gegenüber Subunternehmern gelten, dass ein der DSGVO entsprechendes Schutzniveau gewährleistet ist. Die Parteien stellen klar, dass daraus keine Verpflichtung des Anbieters folgt, die Regelungen dieses Auftragsverarbeitungsvertrags wortgleich auch dem Subunternehmer aufzuerlegen. Werden

mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

(4) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(5) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(6) Der Anbieter haftet gegenüber dem Kunden dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Anbieter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(7) Die jeweils aktuelle Liste der Subunternehmer des Anbieters ist unter https://meisterplan.com/de/subunternehmer/ abrufbar. Mit deren Beauftragung erklärt sich der Kunde einverstanden.

(8) Der Anbieter kann gemäß Art. 28 Abs. 2 Satz 2 DSGVO weitere Subunternehmer hinzuziehen. In diesem Fall informiert der Anbieter den Kunden 30 Tage bevor Daten mit dem neuen Subunternehmer geteilt werden. Anschließend erweitert der Anbieter die unter https://meisterplan.com/de/subunternehmer/ abrufbare Liste. Insoweit wird auch klargestellt, dass der Kunde nur dann informiert wird, wenn Subunternehmer hinzugezogen werden, die Zugriff auf die personenbezogenen Daten des Kunden erhalten.

(9) Sollte der Kunde innerhalb von 30 Tagen nach Erhalt der Information berechtigte Einwände gegen die Einsetzung eines neuen Unterauftragnehmers vorbringen, werden die Parteien nach Treu und Glauben zusammenkommen, um eine angemessene Lösung zu erörtern. Wenn eine solche Lösung nicht erreicht werden kann, kann der Kunde die Vereinbarung kündigen und erhält eine anteilige Rückerstattung der Nutzungsvergütung.

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Im Anhang 1 („Technische und organisatorische Maßnahmen“) sind die diesbezüglichen technischen und organisatorischen Maßnahmen des Anbieters aufgeführt.

(3) Die Maßnahmen des Anbieters können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(4) Wesentliche Änderungen muss der Anbieter mit dem Kunden in dokumentierter Form (schriftlich, elektronisch) abstimmen, soweit sie eine Auswirkung auf die Erbringung des Service haben. Solche Abstimmungen sind für die Dauer dieses Auftragsverarbeitungsvertrages aufzubewahren.

§ 10 Verpflichtungen des Anbieters nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

(1) Nach Abschluss der vertraglichen Arbeiten hat der Anbieter sämtliche vom Kunden zur Verarbeitung überlassenen Anwendungsdaten zu löschen.

(2) Dies wird erreicht über die automatische Löschung der Anwendungsdaten nach Ablauf einer Frist von dreißig (30) Tagen nach Beendigung des Vertragsverhältnisses. Wegen der Einzelheiten wird auf die Regelungen des § 14 des Servicevertrages (Teil I dieser Bedingungen) verwiesen.

§ 11 Haftung

Auf Art. 82 DSGVO wird verwiesen.

Anlage 1: Technische und organisatorische Maßnahmen

Folgende technisch-organisatorische Maßnahmen werden von dem Anbieter im Bereich Meisterplan realisiert.

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

1. Jeder Anwender-Zugang zu Datenverarbeitungsanlagen und Systemen ist nur über eine Benutzerkennung mit Passwort oder über eine SSO-Lösung möglich.
2. Kennwortrichtlinie laut Active-Directory Richtlinie.
3. Zugang zum zentralen Kundenmanagement-System ist über Single-Sign-On (SSO) an das Benutzerkonto des Mitarbeiters gekoppelt.
4. Art des Zugriffs wird über abgestufte Benutzerberechtigungen erstellt und verwaltet.
5. Bildschirmsperrung nach 5 Minuten Inaktivität, per Benutzerrichtlinie.
6. VPN-Zugang an ausgewählte Mitarbeiter von extern zum Firmennetzwerk.
7. Chipkarten-Schließsystem und Sicherheitsschlösser.
8. Kontrollierte Vergabe, Einzug und Sperrung der Chipkarten.
9. Eingangskontrolle am Empfang.
10. Jede Gebäudeebene ist getrennt durch Chipkartenzugang gesichert.
11. Besucherausweise für personalisierten, temporären Zugang zum Gebäude.
12. Kameraüberwachung Einfahrt und Eingang Tiefgarage.
13. Alarmanlage Tiefgarageneingang des Anbieters.
14. Serverräume sind nur für Mitarbeiter der Abteilung IT und für die Geschäftsführung zugänglich und gesondert gesichert.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. 2-Faktor Authentifizierung bei Passwortmanagement-Software und bei Hosting-Provider Amazon Web Services (AWS).
2. Es werden nur sichere Passwörter zu Applikationen erlaubt, welche in einer Passwortmanagement-Software verwaltet werden.

3. Administrative Zugriffe auf die AWS-Konsole werden geloggt.

   Für Sicherheitsrichtlinien des Rechenzentrums bei AWS siehe https://aws.amazon.com/de/compliance/data-center/controls/

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

1. Sichtschutzfolien für Notebooks von Mitarbeitern, welche an öffentlichen Plätzen arbeiten.
2. Clean-Desk Policy.
3. Festplatten von Notebooks / Laptops sind verschlüsselt.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Bei Meisterplan werden keine Datenträger an Dritte verschickt oder von Dritten empfangen. Der Austausch von Daten findet ausschließlich mittels Filesharing-Plattform mit Rechte- und Löschkonzept und gesicherter Verbindung statt.
2. Der Einsatz von USB-Sticks, um Kundendaten zu verarbeiten, ist bei Meisterplan nicht erlaubt.

Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

1. Jeder Anwender-Zugang zu Datenverarbeitungsanlagen und Systemen ist nur über eine Benutzerkennung mit Passwort oder über eine SSO-Lösung möglich.
2. Zugang zum zentralen Kundenmanagement-System ist über SSO an das Benutzerkonto des Mitarbeiters gekoppelt.
3. Im zentralen Kundenmanagement-System werden die Zugriffe auf das System und Datenänderungen protokolliert.
4. Die Änderungen an Benutzerberechtigungen zentralen Kundenmanagement-System in der Administrationsoberfläche werden manuell protokolliert.
5. Die Art des Zugriffs wird über abgestufte Benutzerberechtigungen erstellt und verwaltet.
6. Bildschirmsperrung nach 5 Minuten Inaktivität am Arbeitsplatzrechner per Benutzerrichtlinie.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Die Test-Daten sind getrennt von den Produktiv-Daten. Im Detail heißt das, dass das Meisterplan Continuous Integration Cluster getrennt ist vom Produktiv-Cluster.
2. Die Backups von Meisterplan Anwendungsdaten werden ausschließlich verschlüsselt transportiert/gespeichert. Die Backups werden in der jeweiligen Region (USA / Deutschland) gespeichert.
3. Anwendungsdaten dürfen nur nach Einwilligung des Kunden zur Fehler-Reproduktion oder Beratungszwecke verwendet werden. Nach Zweckerfüllung werden Datenkopien unwiderruflich gelöscht.
4. Der Datentransfer wird ausschließlich verschlüsselt vorgenommen.

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

1. Jeder Anwender-Zugang zu Datenverarbeitungsanlagen und Systemen ist nur über eine Benutzerkennung mit Passwort oder über eine SSO-Lösung möglich.
2. Zugang zum zentralen Kundenmanagement-System ist über SSO an das Benutzerkonto des Mitarbeiters gekoppelt.
3. Im zentralen Kundenmanagement-System werden die Zugriffe auf das System und Datenänderungen protokolliert.
4. Die Änderungen an Benutzerberechtigungen im zentralen Kundenmanagement-System in der Administrationsoberfläche werden manuell protokolliert.
5. Die Art des Zugriffs wird über abgestufte Benutzerberechtigungen erstellt und verwaltet.
6. Bildschirmsperrung nach 5 Minuten Inaktivität am Arbeitsplatzrechner per Benutzerrichtlinie.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Regelmäßige Revision der Zugriffsberechtigungen auf interne Meisterplan-Anwendungen (JIRA, Stash etc.).
2. Auf die Meisterplan AWS Produktiv-Infrastruktur haben nur ausgewählte, langjährige, speziell ausgebildete und vertrauenswürdige Mitarbeiter des Anbieters Zugriff. Es existiert ein Prozess zum Auswahlverfahren.
3. Administrationszugriffe auf die Meisterplan AWS-Dienste werden protokolliert.
4. Änderungen am Deployment der Meisterplan-Anwendungen werden über Code-Versionierung protokolliert.

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

1. Toolgestütztes Passwortmanagement in allen Bereichen.
2. Alle firmeninternen Anwendungen, die durch einen Browser außerhalb des internen Netzwerkes aus dem Internet erreichbar sind, haben TLS geschützte Verbindungen.
3. Schutz vor unberechtigtem Zugriff durch Einsatz von Virenschutz und Firewall.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Die Benutzerrechte der Mitarbeiter richten sich nach dem jeweiligen Aufgabenbereich des Mitarbeiters („need-to-know"-Prinizip).
2. SSO für Meisterplan-Kunden wird angeboten.
3. Der integrierte Authentifizierungsservice von Meisterplan stellt sicher, dass auf Kundendaten nur durch den Kunden und nicht durch andere Personen zugegriffen werden kann.

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

1. Datentransfer nur über verschlüsselte Verbindung
2. Einsatz von VPN

Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

1. Im zentralen Kundenmanagement-System werden die Zugriffe auf das System und Datenänderungen auf Benutzerebene protokolliert.

Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

1. Es erfolgt kein Transport von physischen Datenträgern mit unverschlüsselten Daten Dritter innerhalb von itdesign oder zu Auftragnehmern von itdesign.
2. Datenträger in Notebooks sind verschlüsselt und mit einem Passwort gesichert.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Bei Meisterplan werden keine Datenträger an Dritte verschickt oder von Dritten empfangen. Der Austausch von Daten findet ausschließlich mittels Filesharing-Plattform mit Rechte- und Löschkonzept und gesicherter Verbindung statt.
2. Der Einsatz von USB-Sticks um Kundendaten zu verarbeiten ist bei Meisterplan nicht erlaubt.
3. Der Zugriff auf Anwendungsdaten über Web-Protokolle oder SSH erfolgt ausschließlich verschlüsselt.

Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

1. Backup- und Recoverykonzept
2. Kontrolle des Backupvorgangs
3. Verwendung eines RAID-Systems/Festplattenspiegelung

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Automatisierte Wiederherstellung von Cloud Computing-Ressourcen bei Ausfall.

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

1. Akustische Warnmeldung bei Fehlfunktion USV / Server
2. Automatische Benachrichtigung bei Systemausfall
3. Redundante Stromversorgung aller produktiven Server
4. Jährliche Unterweisung der Mitarbeiter zu Datenschutz-Richtlinien
5. Alle Mitarbeiter unterzeichnen eine Erklärung auf das Datengeheimnis (§5 BDSG). Ab 25.05.2018 verpflichten sich die Mitarbeiter zur Vertraulichkeit auf Grundlage Art. 5 Abs. 1 f., Art. 32 Abs. 4 Datenschutz-Grundverordnung (DSGVO).

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Hohe Redundanz der Infrastruktur (Computing, Storage, Network) durch AWS. Dadurch wird eine sehr hohe Verfügbarkeit der Meisterplan-Systeme gewährleistet.
2. Monitoring der Systeme und Infrastruktur erfolgt durch Erfassung diverser Metriken, Auswertung von Logs, Health Checks der Systeme, Alerting-System.
3. Eingerichtete und dokumentierte, hoch verfügbare Rufbereitschaft von 4 Personen (rotierend).
4. Hohe Qualität der Anwendung wird sichergestellt durch Tests auf allen Ebenen (Unit-Tests, Integrations-Tests, e2e-Tests, UI-Tests, manuelle Tests mit Testplänen). Geschultes Personal in der QS.
5. Incident-Management-Process mit Verbesserungsprozess.
6. Sicherheit ist im Meisterplan-Entwicklungsprozess verankert. Externe Überprüfung erfolgt durch spezialisierten Pen-Test-Dienstleister.

Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

1. Backupkonzept – und Recoverykonzept
2. Kontrolle des Backupvorgangs
3. Monitoring der produktiven Systeme

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

1. Reinigungsdienstleister werden sorgfältig ausgewählt.
2. Mitarbeiter, die im Auftrag eines Verantwortlichen Daten verarbeiten sind über die mit dem Auftraggeber geschlossenen AV-Verträge informiert.
3. Die AV-Verträge sind einschließlich der vereinbarten technisch-organisatorischen Maßnahmen für die mit der Verarbeitung betroffenen Mitarbeiter verfügbar.
4. Die vereinbarten technisch-organisatorischen Maßnahmen werden in wiederkehrenden internen Datenschutzaudits überwacht.

5. Mit allen Subunternehmern, die im Rahmen der Auftragsverarbeitung eingesetzt werden, existieren AV-Verträge.

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

1. Feuerlöschgerät im Serverraum
2. Geräte zur Überwachung von Temperatur und Feuchtigkeit in den Serverräumen
3. Der Serverraum ist klimatisiert.
4. USV-Anlage
5. Das komplette Gebäude ist mit Feuer- und Rauchmeldeanlagen ausgestattet.
6. Aufbewahrung der Datensicherungen an einem sicheren, ausgelagerten Ort.
7. Verwendung eines RAID-Systems / Festplattenspiegelung.

Zusätzlich zu den oben beschriebenen Maßnahmen führt der Anbieter im Bereich Meisterplan für den Kunden noch folgende Maßnahmen durch:

1. Monitoring der Systeme und Infrastruktur durch Erfassung diverser Metriken, Auswertung von Logs, Health Checks der Systeme, Alerting-System.
2. Eingerichtete und dokumentierte, hoch verfügbare Rufbereitschaft von 4 Personen (rotierend).
3. Reporting über Verfügbarkeitsstatistiken liegen vor.
4. Für Sicherheitsrichtlinien des Rechenzentrums bei AWS siehe https://aws.amazon.com/de/compliance/data-center/controls/

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

1. Test-, Entwicklungs- und Produktivsysteme sind technisch voneinander getrennt.
2. Die Zugriffsberechtigungen auf Kunden- und Beschäftigungsdaten werden über Benutzerrechte sowie über logische Trennung (Kennzeichnungen in den Datensätzen) im zentralen Kundenmanagement-System gesteuert.

Weisungsgemäße Verarbeitung

Es ist nach und Art. 32 Abs. 4 DSGVO dafür Sorge zu tragen, dass Mitarbeiter und externe Dienstleister, die Zugang zu personenbezogenen Daten haben, diese nur entsprechend den Weisungen des Verantwortlichen verarbeiten. Hierzu werden nachfolgende Maßnahmen ergriffen:

1. Verpflichtung der Mitarbeiter auf das Datengeheimnis
2. Umsetzung von eigenen Sicherheitsrichtlinien
3. Schulungen

Datenschutzmanagement

Folgende zusätzliche Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung werden nach Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO eingesetzt

4. Datenschutz-Management nach der PDCA-Methode
5. Incident-Response-Management
6. Datenschutzfreundliche Voreinstellungen nach Artikel 25 Absatz 2 DSGVO