

Vertrag über die Verarbeitung von Daten im Auftrag

Zwischen

Firmenname

Anrede, Vorname, Nachname des Ansprechpartners

Straße, Hausnummer

PLZ, Ort

- nachfolgend **Auftraggeber** genannt -

und

NETZWERKZEUG GmbH
Zwickauer Str. 25
D-08393 Meerane

- nachfolgend **Auftragnehmer** genannt -

wird folgende Vereinbarungen über eine Auftragsverarbeitung im Sinne des Art. 28 Abs. 3 der Datenschutz-Grundverordnung (im Folgenden DS-GVO genannt) geschlossen:

Präambel

Diese Vereinbarungen finden Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend Daten) des Auftraggebers verarbeiten.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag vom _____, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung) sowie alle im Zusammenhang mit der Leistungsvereinbarung stehenden ergänzenden Aufträge. Die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sind in der Anlage 1 zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
- (2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.
- (3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
- (4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
- (5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
- (6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
- (7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
- (2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail) erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 - 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.
- (3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragmäßige Abwicklung aller vereinbarten Maßnahmen zu.
- (4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.
- (5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des

Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern z.B. im Home-Office und/oder Privatwohnungen wird zugestimmt, wenn sichergestellt ist, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ des Auftragnehmers gewährleistet sind. Siehe „Home-Office“-Regelung

(9) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(10) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage 4 benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen. Die aktualisierte Liste kann der Auftraggeber über <https://netzwerkzeug.com/avv/> herunterladen.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Die Kontaktdaten des Datenschutzbeauftragten sind in der Anlage 4 benannt. Der Auftragnehmer hat den Auftraggeber über Änderungen oder Wegfall des Datenschutzbeauftragten gesondert in Textform mitzuteilen.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- 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;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. „Home-Office“-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office“ verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office“ durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office“ eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle im „Home-Office“ von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. Unterauftragsverhältnisse

- (1) Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragnehmer) hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsabschlusses hinzugezogenen weiteren Unterauftragnehmer ergeben sich aus der Anlage 2. Die aktualisierte Liste kann der Auftraggeber über <https://netzwerkzeug.com/avv/> herunterladen. Generell nicht genehmigungspflichtig sind Dienstleister, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.
- (2) Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Einsetzung weiterer Unterauftragsnehmer informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Unterauftragsnehmers zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.
- (3) Der Vertrag zwischen dem Auftragnehmer und dem weiteren Unterauftragsnehmer muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Unterauftragsnehmers die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.
- (4) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.
- (5) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.
- (6) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.
- (7) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
- (8) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.
- (9) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Bei der Wartung und Pflege von IT-System oder Applikationen die

vom Auftragnehmer als Unterauftragsverhältnis vergeben werden stellen eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

(4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12-23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

13. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

14. Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

15. Technische und organisatorische Maßnahmen zur Datensicherheit

- (1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
- (2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
- (3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

16. Dauer des Auftrags

- (1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.
- (2) Die Dauer dieses Auftrags (Laufzeit) entspricht mindestens der Laufzeit der Leistungsvereinbarung.
- (2) Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar.
- (3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

17. Beendigung

- (1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.
- (2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.
- (3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

18. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

19. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(Datum der eSignatur, eSignatur Auftraggeber)

(eSignatur NETZWERKZEUG GmbH, Auftragnehmer)



NETZWERKZEUG GmbH
Geschäftsführer: Ralf Kohl
Amtsgericht Chemnitz, HRB 35104

Zwickauer Str. 25
D-08393 Meerane
<https://netzwerkzeug.com>

Anlage AVV 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Vertragsgegenstand ist die entgeltliche Bereitstellung einer Software durch den Auftragnehmer, die dem Auftraggeber auch als Software zur Kommunikation mit seinen Kunden (Dritte) dienen kann. Zudem bietet die Software dem Auftraggeber die Möglichkeit, für Dritte einen digitalen Vertragsordner anzulegen, mit Hilfe derer diese Dritten Informationen zu ihren Verträgen und freigegebene Dokumente einsehen und eigenständig anlegen / verwalten können.

2. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Administratordaten (Ansprechpartner im Unternehmen)
- Mitarbeiterdaten des Unternehmens
- Kunden und Interessenten des Unternehmens
- Endkunden (z.B. Versicherungsnehmer)
- Angehörige der Endkunden
- Mitversicherte Personen
- Bezugsberechtigte Personen
- Bevollmächtigte Personen
- Notfallkontakte
- Kooperationspartner
- Kooperationspartner-Mitarbeiterdaten
- Kunden und Interessenten der Kooperationspartner
- Webseitenbesucher
- Interessenten

3. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten (Anrede, Vorname, Nachname, Geschlecht, Geburtsdatum, Anschrift)
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten in folgenden Kategorien (inkl. zugehöriger Dokumente und Unterlagen):
 - Versicherungen
 - Finanzanlagen (z.B. Bank- und Depotkontendaten)

- Vollmachten und Verfügungen
- Sonstige Verträge (z.B. Gas, Strom, Mobilfunk, Miete)
- Sonstige nicht spezifizierte Vertragsstammdaten (z.B. Renten- und Sozialversicherungsnummer)
- Nutzungsdaten, wie IP-Adressen und Browsertyp und -version

Anlage AVV 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Unterauftragnehmer	Auftragsgegenstand
1&1 IONOS SE Elgendorfer Str. 57, D-56410 Montabaur Telefon: +49 721 170 5522 E-Mail: info@ionos.de	Domain-Services E-Mail-Postfächer
Bispino IT GmbH Friedrichstr. 5, D-36037 Fulda Telefon: +49 661 206 022 61 E-Mail: mail@bispino.com	IT-Dienstleistung Einrichtung, Wartung, Pflege, Programmierung, Support
Contabo GmbH Aschauer Straße 32a, D-81549 München Telefon: +49 89 3564717 70 E-Mail: info@contabo.com	Server-Hosting
synaforce GmbH IT-Zentrum 1, D-94544 Hofkirchen Telefon: +49 8545 96 99 30 E-Mail: info@synaforce.com	Infrastructure as a Service Hosting der technischen Infrastrukturen (Server, Datenbanken) Technischer 3rd-Level Support
Zoho Corporation GmbH Trinkausstr. 7, D-40213 Düsseldorf Telefon: +49 800 0229966 E-Mail: Zoho.Deutschland@eu.zohocorp.com	CRM/ERP auf europäischen Servern von zoho.eu

Anlage AVV 3 - Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

§ 1 Vertraulichkeit /Art. 32 Abs. 1 lit. B DS-GVO)

(1) Zutrittskontrolle

Die Haustür ist immer abgeschlossen. Unbefugten und insbesondere betriebsfremden Personen ist der Zugang grundsätzlich verwehrt; er kann erst nach ausdrücklicher Freigabe durch einen Mitarbeiter unter Benennung des Anlasses ermöglicht werden. Es erfolgt ein kontrollierter Einlass von Besuchern nach Klingelzeichen. Besucher werden am Empfangsbereich abgeholt und bis zum gewünschten Ziel begleitet.

Es existieren sowohl Sicherheitsschlösser wie auch eine Schlüsselregelung.

(2) Zugangskontrolle

Der Schutz vor unbefugter Systemnutzung wird gewährleistet mittels Zugriffsbeschränkung über VPN und SSL-Tunnel.

Der Zugang zur technischen Arbeitsumgebung ist durch Benutzername und Passwort geschützt. Es existiert eine Passwort-Richtlinie. In diesem Zusammenhang wird eine gewisse Passwortlänge- und Komplexität gefordert sowie das Benutzerkonto nach einer vorgegebenen Anzahl von Falschanmeldungen gesperrt.

Nicht mehr benötigte Zugangsberechtigungen werden zeitnah entzogen.

Der Arbeitsplatzrechner wird nach einer vorgegebenen Zeitdauer der Inaktivität gesperrt.

Die Arbeitsplatzrechner sind durch Anti-Viren-Software und Firewall geschützt.

(3) Zugriffskontrolle

Es sind ausschließlich Personen, die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Auftragsverarbeitung betraut sind, berechtigt, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen. In diesem Zusammenhang bestehen klare Regelungen zur Vergabe von Zugriffsberechtigungen, die einen differenzierten Zugriff (lesen, ändern, löschen) berücksichtigen und den Zugriff auf den verschiedenen Ebenen regeln.

Um unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten zu verhindern werden entsprechende Berechtigungskonzepte eingesetzt. Darüber hinaus wird der Datenbankzugriff auf eigene bzw. freigegebene Daten beschränkt. Fehlgeschlagene Anmeldeversuche als auch widerrechtliche Modulzugriffe werden protokolliert, um den Versuch einer technischen Kompromittierung frühzeitig zu identifizieren. Im Falle einer Identifikation eines Kompromittierungsversuchs werden betroffene Nutzer gesperrt und der Zugang zur Applikation verwehrt.

Für eventuelle Fernadministration sind Sicherheitsregeln in Kraft.

Zum Schutz gegen einen Zugriff aus nicht vertrauenswürdigen Netzwerken (z.B. Internet) wird eine Firewall eingesetzt.

(4) Trennung

Um die getrennte Verarbeitung von Daten zu gewährleisten, bietet die bereitgestellte Infrastruktur eine Mandatenfähigkeit und begrenzt den Datenzugriff automatisiert gemäß den Berechtigungen des zugreifenden Benutzers.

Es erfolgt ferner eine physikalische Unterscheidung zwischen Produktiv- und Testsystem.

(5) Pseudonymisierung & Verschlüsselung

Eine Pseudonymisierung der Daten wird nicht vorgenommen.

Es erfolgt eine Verschlüsselung der Übertragungswege via VPN oder TLS-/SSL-Verschlüsselung.

§ 2 Integrität (Art. 32 Abs. 1 lit. B DS-GVO)

(1) Eingabekontrolle

Die Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, erfolgt mittels einer entsprechenden Historisierung.

(2) Weitergabekontrolle

Unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport wird mittels einer Ende-zu-Ende Verschlüsselung „Transport-Layer-Security“ (kurz TLS) sichergestellt. Der Server kann über Domain-Validierte SSL-Zertifikate eindeutig identifiziert werden.

§ 3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DS-GVO)

Alle wichtigen Unternehmensdaten werden mehrfach täglich gesichert. Die Wiederherstellung der Datensicherung wurde geprüft. Ständige Dokumentation der Datensicherung.

Zur Gewährleistung der Sicherheit wird die vertraglich vereinbarte Lösung über Rechenzentrum der Klasse „Reliable Data Center CAT III“ bereitgestellt.

- ISO/IEC 27001 / 9001 zertifiziertes Datacenter
- 24 x 7 Überwachung und Rufbereitschaft durch interne Mitarbeiter
- 24 x 7 Monitoring der gesamten Infrastruktur
- Vandalismusgeschützter Innenbereich gem. Resistance Class II nach DIN EN 1631
- Brandschutz EI 30 nach EN 1363
- EMV-Grundschutz
- Staub- und Wasserdichtigkeit IP 55 nach IEC 60 529
- redundante N+1 Switches, Router und Firewalls
- redundante Internetanbindung über 2 Wege und 2 Internet-Provider (IP-Transit)
- EVU Einspeisungen über 2 Wege (1 MW) / Redundante Notstromversorgungen (1 MW)
- Redundante USV-Anlagen
- RAS Anlagen (Brandfrüherkennung)
- Automatische Gaslöschanlage
- Kameraüberwachung mit Aufzeichnung
- Elektromagnetisches Zutrittssystem
- 64 und 9 Racks mit redundanten Strom- und Netzanschlüssen, Energie- und Differenzstrom Messung und Sensorik (Temp. und Luftfeuchte)
- Netzwerk Backbone 7,2 TB/s
- Mehrfach redundante Internetanbindung

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DS-GVO; Art. 25 Abs. 1 DS-GVO)

Alle Mitarbeiter des Unternehmens wurden im Datenschutz unterwiesen. Es liegt von allen Mitarbeitern eine unterschriebene Vertraulichkeitsverpflichtungserklärung vor.

Anlage AVV 4 - Datenschutzbeauftragter, Weisungsberechtigte, Weisungsempfänger

Datenschutzbeauftragter

Der Auftragnehmer hat einen Externen Datenschutzbeauftragten bestellt.

Vorname Nachname	E-Mail:
Olaf Eugling	datenschutz@netzwerkzeug.com
Am Sportplatz 7, D-98530 Dillstädt	

Zuständige Datenschutzbehörde:

Postanschrift:
Sächsische Datenschutzbeauftragte
Postfach 11 01 32
D-01330 Dresden

Hausanschrift:
Sächsische Datenschutzbeauftragte
Devrientstraße 5
D-01067 Dresden

Telefon: +49 351 85471 101
Telefax: +49 351 85471 109

Internet: www.datenschutz.sachsen.de
E-Mail: saechsdsb@slt.sachsen.de

Weisungsberechtigte

Weisungsberechtigt sind auf Seiten des Auftraggebers:

Vorname Nachname	E-Mail:
------------------	---------

Weisungsempfänger

Berechtigt, Weisungen des Auftraggebers zu empfangen, sind:

Vorname Nachname	E-Mail:
Ralf Kohl	admin@netzwerkzeug.com
Elke Motitschke	support@netzwerkzeug.com

Die aktualisierte Liste kann der Auftraggeber über <https://netzwerkzeug.com/avv/> herunterladen.