Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

Auftraggeber (Verantwortlicher):

_____

_____

_____

Auftragnehmer (Auftragsverarbeiter):

Netzwerker-Dresden GmbH

Fritz-Meinhardt-Straße 70

01239 Dresden

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Die Lieferung und Bereitstellung der vereinbarten Leistungen sind im Hauptvertrag geregelt.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags

☒ wird auf unbestimmte Zeit geschlossen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers

nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

☒ Erhebung

☒ Aufzeichnung

☒ Strukturierung

☒ Modifizierung, Anpassung oder Änderung

☒ Speicherung

☒ Updates über Fernwartung

☒ Einsichtnahme

☒ Fehleranalyse und Fehlerbehebung Übertragung

☒ Weitergabe

☒ Netzwerkeinrichtung / Vernetzung

☒ Abgleich

☒ Beschränkung

☒ Abstimmung oder Kombination

☒ Vernichtung

☒ Löschung

☒ Abruf

☒ Sonstige Arten, personenbezogene Daten verfügbar zu machen (z. B. Kommunikation, Nutzung)

_____

_____

_____

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO) und Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

☒ Personenstammdaten	☒ Planungs- und Steuerungsdaten
☒ Vertragsstammdaten	☒ Auskunftsangaben (von Dritte Auskunfteien, oder aus öffentlichen Verzeichnissen)
☒ Kundenhistorie	☐ Gesundheitsdaten
☒ Vertragsabrechnungs- und Zahlungsdaten	☐Soziale Daten
	☐Sonstige Daten
	_____

Betroffene Personen *(Bitte Zutreffendes auswählen)*		
☒ Mitarbeiter	☒ Kunden	☒ Interessenten des Kunden
☒ Behörden	☒ Lieferanten	☒ sonstige Interessenten
☐ keine		

Besondere Kategorien personenbezogener Daten *(Bitte Zutreffendes auswählen)*		
☐ Rassische oder ethnische Herkunft	☐ Politische Meinung	☐ Religion/ Glaube
☐ Philosophische Überzeugungen	☐ Gewerkschaftszugehörigkeit	☐ Genetische Daten
☐ Biometrische Daten	☐ Gesundheitsdaten	☒ Keine
☐ Sexuelle Orientierung	☐ Strafrechtliche Verurteilungen und Straftaten	

Weitere personenbezogene Daten *(Bitte detailliert aufführen)*

_____

_____

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber 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.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungs-empfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:

Weisungsempfänger beim Auftragnehmer sind:

Mitarbeiter Geschäftsleitung, Mitarbeiter Verwaltung, Mitarbeiter Vertrieb, Mitarbeiter First-Level-Support, Mitarbeiter Technik

Für Weisung zu nutzende Kommunikationskanäle beim Auftragnehmer:

E-Mail: info@netzwerker-dresden.de, dispo@netzwerker-dresden.de sowie personifizierte Mailadressen soweit vereinbar.

Post: Netzwerker-Dresden GmbH

Fritz-Meinhardt-Straße 70

01239 Dresden

Der telefonische Kommunikationskanal ist, mit Ausnahme der benannten weisungsberichtigten Personen, ausgeschlossen.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutz-behörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen 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 DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Entsprechend der Definition Art. 32 DS-GVO

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:

E-Mail:

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - 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 Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind (z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.). Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er 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). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

☒ Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz

Beratungshaus

Jens Protze

An der Hauptstraße 4a

04720 Döbeln

Telefon: 0 34 31 – 60 58 28

E-Mail: jens.protze@t-online.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Sofern einschlägig:
Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33

und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

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

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

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen → DS-Audit, Überprüfung der TOM`s usw.

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage „Subunternehmer“ mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen

Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

Gemäß Art. 28 Abs. 4 Satz 2 DS-GVO haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten durch die von ihm eingesetzten Subauftragnehmer.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

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 DS-GVO, 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.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:

Risikobewertung im Verarbeitungsverzeichnis

Das im Anhang Kurzfragelist der TOM`s beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das im Anhang TOM`s beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

Folgende Möglichkeit für den Nachweis durch Zertifizierung bestehen:

☒ Die Bewertung des Risikos samt der Auswahl der geeigneten technischen und organisatorischen Maßnahmen des Auftragnehmers wurden/werden am …… durch folgende unabhängige externe Stellen auditiert/zertifiziert gemäß den Regelungen nach Art. 42:

Datenschutzbeauftragter entsprechend Bestellung

Diese vollständigen Prüfunterlagen und Auditberichte können vom Auftraggeber jederzeit eingesehen werden.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

☐ Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

oder

☐ wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:
Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Die Vergütung der Dienstleistungen sind im Hauptvertrag geregelt.

11. Haftung und Vertragsstrafen

Auf Art. 82 und 83 DS-GVO sowie Erwägungsgründe 146 ff. wird verwiesen.

Verstößt der Auftragnehmer gegen diese Vereinbarung und bestimmt - ggf. auch nur teilweise – Zwecke und Mittel der Verarbeitung, so gilt er insoweit als Verantwortlicher i.S.d. DS-GVO (vgl. Art. 28 Abs. 10 DS-GVO)

12. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

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

14. Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist Dresden.

……..
Ort, Datum

…… ……
Auftraggeber Auftragnehmer

Anlage 1: Subunternehmer
Anlage 2: Kurzfrageliste zur DS-GVO
(Technisch-organisatorische Maßnahmen)

Anlage 1: Subunternehmer

Genehmigte Subunternehmer

Die folgenden Unternehmen werden hiermit im Voraus berechtigt, als Subunternehmer des Auftragnehmers Verarbeitungstätigkeiten auszuführen:

Anschrift	**Zweck der Auftragsdatenverarbeitung**
Beratungshaus Jens Protze An der Hauptstraße 4a 04720 Döbeln	Datenschutzbeauftragter
Office Management Fritsche & Mandel GbR Gompitzer Hang 8 01156 Dresden	Erstellung der Finanzbuchhaltung
hp comnet Holm Pfützner Hauptstraße 25 01448 Moritzburg	Dedizierter Support, sowie technische Administration der Netzwerker-Dresden GmbH
SBS Hartmann + Trenner + Richter GmbH Steuerberatungsgesellschaft Hohe Straße 55 01187 Dresden	Erstellung der Jahresabschlüsse
Verschiedene Hard- / Softwarelieferanten der Netzwerker-Dresden GmbH	(Endkundendaten, Lizenzinformationen, Garantie – und Garantieverlängerungen, Direktlieferungen, Projektanfragen)

Anlage 2: Kurzfrageliste zur DS-GVO (Technisch-organisatorische Maßnahmen)

Nr.	Datensicherheitsmaßnahmen des Auftragnehmers	ja	nein	Bemerkungen ggf an Ansprechpartner
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)				
1.0	**Zutrittskontrolle**			
	Kein unbefugter Zutritt zu Datenverarbeitungsanlagen			
1.01	Besitzen Sie elektrische Türöffner?	☒	☐	
1.02	Ist die Schlüsselvergabe in Ihrem Unternehmen geregelt?	☒	☐	
1.03	Haben Sie ein Zutrittskontrollsystem mit Magnet- oder Chipkarten?	☒	☐	
1.04	Gibt es bei Ihnen Pförtner bzw. einen Werkschutz?	☒	☐	
1.05	Werden Alarm- und Videoanlagen eingesetzt?	☒	☐	
1.1	**Zugangskontrolle**			
	Keine unbefugte Systembenutzung			
1.11	Werden bei Ihnen Anforderungen an die Passwörter, z. B. Sicherheit, Länge, Sonderzeichen, regelmäßiger Wechsel, gestellt?	☒	☐	
1.12	Setzen Sie in Ihrem Unternehmen Zwei-Faktor-Authentifizierung ein, z.B. HardwareToken + Kennwort / PIN?	☒	☐	
1.13	Werden bei Ihnen automatische Sperrmechanismen eingesetzt z. B. Bildschirmschoner?	☒	☐	
1.14	Sind alle zugänglichen Datenträger mit personen-bezogenen Daten verschlüsselt?	☒	☐	
1.2	**Zugriffskontrolle**			
	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems			
1.21	Ist in Ihrem Unternehmen ein Berechtigungs-konzept mit differenzierten Profilen, Rollen, Transaktionen und Objekten etabliert?	☒	☐	
1.22	Wird das Need-to-know-Prinzip (bedarfsgerecht) bei der Vergabe der Zugriffsrechte eingehalten?	☒	☐	
1.23	Können die Zugriffsrechte ausgewertet werden?	☒	☐	

1.24	Werden die einzelnen Zugriffe, sei es Kenntnisnahme, Veränderung oder Löschung, protokolliert?	☒	☐

1.3 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

1.31	Werden personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet?	☒	☐
1.32	Besitzt Ihr Berechtigungssystem Mandantenfähigkeit?	☒	☐
1.33	Verfügen Sie über ein Test- und ein Produktionssystem, z.B. Sandboxing?	☒	☐

1.4 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

1.41	Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen?	☐	☒ Änderung geplant

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

2.0 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

2.01	Wird jede elektronische Datenübertragung von personenbezogenen Daten verschlüsselt?	☐	☒ Änderung geplant
2.02	Werden Maßnahmen zur Absicherung des Transports von Datenträgern, z. B. Verschlüsselung von CDs, getroffen?	☒	☐
2.03	Werden elektronische Signaturen eingesetzt? Wenn ja in welchen Fällen?	☒	☐
2.04	Werden virtuelle, private Netzwerke (VPN) eingesetzt?	☒	☐
2.05	Setzen Sie Protokollierungssysteme ein, welche die Weitergabe von Daten überwachen?	☒	☐

2.1 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

2.11	Werden alle Dateneingaben, -veränderungen und -löschungen protokolliert und ausgewertet?	☒	☐
2.12	Verfügen Sie über einem Administrator-Log?	☒	☐
	Werden Dokumentenmanagementsystem eingesetzt?	☒	☐

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

3.0 Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

3.01	Haben Sie eine Backup-Strategie (online/offline; on-site/off-site)?	☒	☐
3.02	Besitzt Ihr Unternehmen eine unterbrechungsfreie Stromversorgung (USV)?	☒	☐
3.03	Setzen Sie Virenschutz und Firewalls ein?	☒	☐
3.04	Wurde ein Notfallplan und entsprechende Meldewege etabliert?	☒	☐
	Wird eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) sichergestellt?	☒	☐

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

4.0 Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers

4.01	Werden alle Maßnahmen zur weisungsgemäßen Auftragsdatenverarbeitung getroffen und entsprechen diese der aktuellen Gesetzeslage?	☒	☐
4.02	Wird ein formalisiertes Auftragsmanagement eingesetzt?	☒	☐

4.1 Datenschutz-Management

	Wird die Rechenschaftspflicht zum Nachweis der Einhaltung der gesetzlichen Grundsätze	☒	☐

und Regelungen, des Stands der Technik und der Aktualität und Wirksamkeit der Maßnahmen durch ein Datenschutz-Management-System sichergestellt?

4.2 Incident-Response-Management

Wird durch organisatorische und technische Maßnahmen / Prozesse sichergestellt, dass erkannte oder vermutete Sicherheitsvorfälle /Angriffe auf die IT-Infrastruktur bzw. Störungen (technische Probleme; Schwachstellen) erkannt und beseitigt werden können?	☒	☐

4.3 Datenschutzfreundliche Voreinstellunggen (Art. 25 Abs. 2 DS-GVO)

Wird durch geeignete technische und organisatorische Maßnahmen sichergestellt, dass in Bezug auf die Menge, den Umfang, der Speicherfrist und der Zugänglichkeit durch Voreinstellungen die Verarbeitung nur für den jeweiligen bestimmten Verarbeitungszweck erfolgen?	☒	☐

Die Richtigkeit der gemachten Angaben wird bestätigt.

Datum, Ort und Unterschrift:

.....

Funktion der unterzeichnenden Person im Auftragnehmerunternehmen:
Geschäftsführer

Auftragnehmer / Firma:
Netzwerker-Dresden GmbH
Fritz-Meinhardt-Straße 70
01239 Dresden

Name des Datenschutzbeauftragten:
Jens Protze

Telefon / E-Mailadresse des Datenschutzbeauftragten:
+49 (34 31) 60 58 28
jens.protze@t-online.de