Vertrag über die Verarbeitung von Daten im Auftrag gem. Art. 28 DS-GVO

Zwischen

nachfolgend „Auftraggeber“

und

Net-Base Computer- & Netzwerktechnik e. K.
Weißerlenstraße 3
79108 Freiburg
vertreten durch: Markus Rödling

nachfolgend „Net-Base“ oder „Auftragnehmer“

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702

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 (DS-GVO). 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 DS-GVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 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 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 können 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 DS-GVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

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.

(3) 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 DS-GVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(4) 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 1 benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DS-GVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

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.

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DS-GVO 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 nach Art. 33, 34 DS-GVO 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 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 DS-GVO. Es gelten die Regelungen von Ziff. 11 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 DS-GVO genannten Pflichten.

8. 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 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 nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

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. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 2 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, 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.

9. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der Anlage 1 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) 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 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DS-GVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DS-GVO 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 Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 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.

(7) 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. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DS-GVO 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.

10. 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.

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

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

11. 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 DS-GVO zu bearbeiten, zu unterstützten. 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 DS-GVO 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.

12. 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.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

14. 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 DS-GVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 2** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

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 einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) 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.

16. Beendigung

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.

17. 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.

18. 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.

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

Ort, Datum	Unterschrift	Ort, Datum	Unterschrift
Auftraggeber		Auftragnehmer	

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702

Anlage 1 – Gegenstand des Auftrags

1. Art(en) der Verarbeitungstätigkeiten

1.1. Onlinedienste

Der Gegenstand des Auftrags ergibt sich aus dem Vertrag zur Bereitstellung eines oder mehreren der folgenden Onlinedienste, welche durch den Auftragnehmer angeboten werden:

☐ **Hosted Exchange**
beinhaltet die folgenden Funktionen: E-Mail, Adressbuch, Kalender, Aufgaben

☐ **NextCloud**
Verschlüsselter Onlinespeicher

☐ **Webhosting**
beinhaltet u.a. die folgenden Funktionen: E-Mail inkl. Webfrontend, FTP, PHP, MySQL, Backup, … . Die Nutzung des Webspace richtet sich nach der vom Auftragnehmer installierten Software

Der Auftragnehmer stellt mit seinem Hosting-Angebot die o.a. Dienste zur Verfügung. **Eine Verarbeitung personenbezogener Daten im Rahmen dieser Leistungen ist ausdrücklich nicht Bestandteil dieses Angebotes**. Allerdings kann es unter Umständen nicht ausgeschlossen werden, dass während Wartungs- oder Servicearbeiten (Hotline, Support) ein Mitarbeiter des Auftragnehmers Kenntnis von personenbezogenen Daten aus dem Verantwortungsbereich des Auftraggebers erlangt.

Für den sicheren Betrieb der Webserver sind außerdem umfangreiche Logmechanismen im Einsatz (FTP-Log, Access-Log, Error-Log). Hierbei werden die folgenden Daten gespeichert:

- Browsertyp und Browserversion
- verwendetes Betriebssystem
- Referrer URL
- Hostname des zugreifenden Rechners
- Uhrzeit der Serveranfrage
- IP-Adresse

Die Logfiles werden ausschließlich zu Konfigurations- und Sicherheitszwecken verwendet und nach 14 Tagen gelöscht.

1.2. IT-Service

Der Gegenstand des Auftrags ergibt sich aus den jeweils beauftragten Dienstleistungen:

☐ PC-, Server- und Netzwerkinstallation, -konfiguration, -vor-Ort Wartung

☐ Installation, Einrichtung, Schulung von Anwendungssoftware

☐ Fernwartung

☐ Reparatur Hardware (Werkstattauftrag)

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

☐ Reparatur Hardware (RMA – Sendung an Lieferant / Hersteller)

☐ Entsorgung Hardware / Datenträger

☐ Sonstiges (bitte spezifizieren)

Der Auftragnehmer bietet mit seinem Serviceangebot die o.a. Dienstleistungen an. Eine Verarbeitung personenbezogener Daten im Rahmen dieser Leistungen ist ausdrücklich nicht Bestandteil dieses Angebotes. Allerdings kann es unter Umständen nicht ausgeschlossen werden, dass während Wartungs- oder Servicearbeiten (Hotline, Support) ein Mitarbeiter des Auftragnehmers Kenntnis von personenbezogenen Daten aus dem Verantwortungsbereich des Auftraggebers erlangt.

2. Kategorien personenbezogener Daten

Folgende Datenarten sind unter Umständen einsehbar:

☐ Name / Vorname
☐ Adresse
☐ E-Mail Adresse
☐ Telefonnummer
☐ Vertragsdaten
☐ Kontodaten
☐ Steuerdaten
☐ Sozial- / Versicherungsdaten
☐ Gesundheitsdaten
☐ Konfessionsdaten
☐ Vertragsdaten
☐ Sonstiges (bitte unten spezifizieren)

3. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

☐ Kunden / Interessenten
☐ Lieferanten
☐ Beschäftigte i.S.d. § 26 (8) BDSG neu
☐ Sonstige (bitte spezifizieren)

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702

4. Weisungsberechtigte Personen des Auftraggebers

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

6. 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(s) Unternehmen:

Für die Entsorgung von Datenträgern

Rhenus SE & Co. KG

Rhenus-Platz 1

59439 Holzwickede

Betrieb und Wartung von Starface Telefonlösungen

Starface GmbH

Stephanienstraße 102

76133 Karlsruhe

Fernwartung und -support

TeamViewer Germany GmbH

Jahnstraße 30

73037 Göppingen

Weitere Unterauftragnehmer

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702

Sonderfall Reparatureinsendungen

Im Rahmen einer RMA-Abwicklung wird defekte Hardware u.U. an den Hersteller / Lieferanten zurückgesandt. Sofern es sich Datenträger oder Geräte mit eingebauten Datenträgern handelt, kann es nicht ausgeschlossen werden, dass der Hersteller / Lieferant Kenntnis von den darauf gespeicherten Daten erhält.

Hierbei besteht i.d.R. kein Untervertragsverhältnis zur Auftragsverarbeitung mit dem jeweiligen Hersteller / Lieferanten.

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702

Anlage 2 – Sicherheit der Verarbeitung – unsere TOMs

Für unsere Online-Dienstleistungen: Rechenzentrum Freiburg

Die nachfolgend beschrieben Maßnahmen entsprechen dem „Stand der Technik“ (technische Maßnahmen die erhoben werden, die zur Verfügung stehen und die sich bereits in der Praxis bewährt haben).

Vertraulichkeit	
Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen	• Von innen vollverschalte, einbruchshemmende Fenster, öffnen nicht möglich (Einbruch- und Klimaschutz) • einbruchhemmende Türen • Zutritt über Telenot-System gesichert • Zutritt nur mit Schlüssel (Vorraum) und personalisierten Badges (Serverraum) • EMA (Einbruchmeldeanlage)
Zugangskontrolle Keine unbefugte Systembenutzung	• Abgeschlossenen Server-Racks • Alle Systeme sind passwortgesichert • Serverraum videoüberwacht
Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen	• Der Zugriff auf die Serversysteme ist ausschließlich dazu ausgebildeten und autorisierten Mitarbeitern von Net-Base mit den entsprechenden Zugangsdaten möglich • Wartungsarbeiten finden auf Systemebene statt, ein Zugriff auf Kundendaten erfolgt hierbei nicht • Zugriffe auf Kundensysteme erfolgen ausschließlich nach Weisung und Auftrag des Auftraggebers
Trennungskontrolle Getrennte Verarbeitung von Daten, die unterschiedlichen Zwecken dienen	• Die Internet-Präsenzen und sonstigen Online-Dienstleistungen werden über speziell dafür vorgesehene Software zur Verfügung gestellt. Zentraler Bestandteil ist hierbei die Trennung der verschiedenen Datenbestände • Zugriff erhält der Auftraggeber ausschließlich zu seinen gebuchten Paketen • Kundennetze sind grundsätzlich logisch getrennt (VLAN)
Pseudonymisierung	• Maßnahmen zur Pseudonymisierung werden ausschließlich in Zusammenarbeit mit unseren

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

	Kunden auf deren Wunsch anforderungsbezogen umgesetzt.
Verschlüsselung	• Alle Cloudserver sind auf Filesystemebene verschlüsselt. Der Zugriff ist ausschließlich (mit vom Kunden bereitgestellten) Benutzer- oder Admin-Accounts möglich.
	Integrität
Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	• Zugriffe von extern für technische / administrative Aufgaben finden ausschließlich über verschlüsselte Verbindungen statt (TLS-ranking der Net-Base Server: A+ Quelle: www.ssllabs.com) • Die Verantwortung für eine gesicherte Übertragung auf Webserverebene liegt beim Auftraggeber und wird von Net-Base im Bedarfsfall eingerichtet • Alle Mitarbeiter von Net-Base sind im Umgang mit personenbezogenen Daten sensibilisiert und schriftlich auf Verschwiegenheit u.a. gem. § 88 TKG verpflichtet
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Systeme eingegeben, verändert oder entfernt worden sind	• Systemzugriffe werden grundsätzlich geloggt und nach 14 Tagen gelöscht • Erfolglos versuchte Zugriffe werden geloggt und automatisiert geblockt
	Verfügbarkeit und Belastbarkeit (Resilienz)
Verfügbarkeitskontrolle Rasche Wiederherstellbarkeit: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	• Redundante Klimatechnik mit regelmäßigen Wartungsintervallen • Doppelboden-Klimatisierung • Redundante USV-Anlage für kurzzeitige Ausfälle und Spannungsspitzen mit regelmäßigen Wartungsintervallen • Dieselaggregat für längere Stromausfälle (12 Stunden unter Voll-Last, nachtankbar im laufenden Betrieb) mit regelmäßigen Wartungsintervallen • Brandschutz F90 für Türen und Wände • Brandfrüherkennung und BMA (Brandmeldeanlage) mit Feuerwehraufschaltung mit regelmäßigen Wartungsintervallen • 24/7/365 Überwachung der Infrastruktur durch

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

	externes NOC (Network Operation Center) • Regelmäßige Aktualisierung der Serversoftware • Serverbasierter Viren- und Schadsoftwareschutz • Datensicherung: Tägliches Backup mit einer Vorhaltezeit von 30 Tagen
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	
	• Regelmäßige Recoverytests • interne Audits der Maßnahmen werden regelmäßig gemeinsam mit den Beteiligten durchgeführt. Diese Audits sind Bestandteil der Auditplanung im Rahmen unseres QMS • Backups werden gemonitored und täglich auf korrekte Durchführung geprüft • Die Server-Infrastruktur wird über verschiedene Mechanismen auf Funktionsfähigkeit und unerlaubte Zugriffe hin überwacht • Zur ständigen Verbesserung unserer Abwehrmechanismen und Spamschutzmaßnahmen ist ein Honeypot im Einsatz • Honeypot-Angriffe werden umgehend und direkt an das BSI gemeldet, Angriffe (DDoS, Bruteforce auf diverse Dienste) werden an die jeweiligen Netzbetreiber gemeldet • Spezifische Schutzmaßnahme könne auf Kundenanforderung implementiert werden

Für unsere IT-Dienstleistungen: Firmengebäude Net-Base

Die nachfolgend beschrieben Maßnahmen entsprechen dem „Stand der Technik“ (technische Maßnahmen die erhoben werden, die zur Verfügung stehen und die sich bereits in der Praxis bewährt haben).

Vertraulichkeit	
Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen	• Kontrollierter Eingangsbereich während der Geschäftszeiten • Durchgangsmelder / Videoüberwachung • Schlüssel und Transponder • Schlüsselregelung • Bewegungsmelder • EMA (Einbruchmeldeanlage) mit Direktaufschaltung Wachdienst

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

Zugangskontrolle Keine unbefugte Systembenutzung	• Eigener Serverraum, fensterlos • Der Zugang zu den IT-Systemen ist ausschließlich berechtigten (mit einem entsprechenden Login ausgestatten) Personen möglich. Jeder Mitarbeiter sperrt seinen Bildschirm beim Verlassen des Arbeitsplatzes. • Die IT-Systeme sind nach außen hin mit einer Firewall gegen unberechtigte Zugriffe geschützt. Die Firewall-Regeln werden permanent aktualisiert. • Sämtliche Serversysteme werden darüber hinaus durchgängig per Monitoring Software überwacht: • Das getrennt installierte W-LAN-Netz wird nach WPA2/SPK verschlüsselt und bietet keinen Zugang zum restlichen Firmennetzwerk. • Reinigungspersonal hat ausschließlich während der Arbeitszeit Zutritt zu den Räumen.
Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen	• Der Zugriff auf die Serversysteme ist ausschließlich dazu ausgebildeten und autorisierten Mitarbeitern von Net-Base mit den entsprechenden Zugangsdaten möglich • Wartungsarbeiten finden auf Systemebene statt, ein Zugriff auf Kundendaten (ERP) durch Administratoren oder Benutzer erfolgt hierbei nicht • Keine Kundenapplikationen und Hostingpakete in diesen Räumen
Trennungskontrolle Getrennte Verarbeitung von Daten, die unterschiedlichen Zwecken dienen	• Getrennte Netze für W-LAN, Kunden, Office und Technik • Getrennte Laufwerkszugriffe auf Domänenebene • Getrennte Zugriffsrechte auf ERP-Systemebene • Reparaturgeräte nur in separatem Netz / Kennzeichnung Kundengeräte im Rahmen unseres QMS
Pseudonymisierung	• Maßnahmen zur Pseudonymisierung werden ausschließlich in Zusammenarbeit mit unseren Kunden auf deren Wunsch anforderungsbezogen umgesetzt.
Verschlüsselung	• Unsere Websites sind SSL-verschlüsselt • Wir kommunizieren über signierte Mails und

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

	können unseren Kunden verschlüsselte E-Mail-Kommunikation anbieten, sofern dies kundenseitig technisch möglich und gewollt ist • Vertrauliche Daten werden nach Absprache als verschlüsselte Datei verschickt • Geräte im Außeneinsatz (Smartphone, Notebooks) sind verschlüsselt • Zugänge von extern erfolgen ausschließlich über verschlüsselte VPN-Verbindungen
Integrität	
Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport	• Siehe oben „Verschlüsselung“ • Login für Beschäftigte ausschließlich über personalisierte Domänenbenutzerkontos • Need-to-know Prinzip bei der Rechtevergabe • Login ggf. zusätzlich auf Applikationsebene • Passwortmanagement über verschlüsselt abgelegte Passwortmanager
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Systeme eingegeben, verändert oder entfernt worden sind	• Systemzugriffe werden grundsätzlich geloggt und nach 14 Tagen gelöscht • Erfolglos versuchte Zugriffe werden geloggt und automatisiert geblockt • Eingabekontrolle auf ERP-Ebene • Fernwartungstätigkeiten per Teamviewer werden protokolliert
Verfügbarkeit und Belastbarkeit (Resilienz)	
Verfügbarkeitskontrolle Rasche Wiederherstellbarkeit: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	• Klimaanlage im Serverraum mit regelmäßigen Wartungsintervallen • USV-Anlage für kurzzeitige Ausfälle und Spannungsspitzen mit regelmäßigen Wartungsintervallen • Durch einen entsprechenden Sensor wird der Serverraum auf die folgenden Parameter hin überwacht: Temperatur Feuchtigkeit Rauch • Das Netzwerk wird durch eine Firewall gegen Angriffe von außen geschützt. • Die Server werden durch den Einsatz von

Net-Base Computer- und Netzwerktechnik e.K. www.net-base.de
Weißerlenstraße 3 +49 (0) 761 - 50 453-0 Sitz des Unternehmens: Freiburg USt-IdNr.: DE156588612
79108 Freiburg info@net-base.de Handelsregister: AG Freiburg HRA 700570 WEEE-Reg.-Nr.: DE69729702

	entsprechender Software überwacht. Alarmmeldungen werden direkt auf das Handy der Geschäftsleitung und der Administratoren weitergeleitet. • Die Administratoren sorgen für ein kontrolliertes Update / Patch-Management der Serversoftware. • Zum Schutz vor Schadsoftware wird eine Antivirus-Software netzwerkweit eingesetzt. Das Updatemanagement wird serverseitig durchgeführt. • Die Datensicherung erfolgt durch entsprechende Backup-Software und wird zusätzlich aushäusig beim Geschäftsführer aufbewahrt. • Die Durchführung der Datensicherung erfolgt automatisiert und wird durch einen Mitarbeiter täglich überwacht.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung	
	• Regelmäßige Recoverytests • interne Audits der Maßnahmen werden regelmäßig gemeinsam mit den Beteiligten durchgeführt. Diese Audits sind Bestandteil der Auditplanung im Rahmen unseres QMS • Backups werden gemonitored und täglich auf korrekte Durchführung geprüft • Die Server-Infrastruktur wird über verschiedene Mechanismen auf Funktionsfähigkeit und unerlaubte Zugriffe hin überwacht • Spezifische Schutzmaßnahme können auf Kundenanforderung implementiert werden

Net-Base Computer- und Netzwerktechnik e.K.
Weißerlenstraße 3
79108 Freiburg
+49 (0) 761 - 50 453-0
info@net-base.de
www.net-base.de
Sitz des Unternehmens: Freiburg
Handelsregister: AG Freiburg HRA 700570
USt-IdNr.: DE156588612
WEEE-Reg.-Nr.: DE69729702