Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

Max Mustermann

Musterstraße 3

54321 Musterstadt

- Verantwortlichen- nachstehend Auftraggeber genannt –

und der

Rapid Data GmbH Unternehmensberatung

Ritterstraße 3, 10969 Berlin
Deutschland / Germany

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

§ 1 Präambel und Geltungsbereich

Der Auftragnehmer erbringt Leistungen für den Auftraggeber aufgrund des Vertrags über Softwarelizenzen, die Bereitstellung webbasierter Lösungen und/oder Dienstleistungen (Leistungsvertrag). Im Rahmen der Leistungserbringung verarbeitet der Auftragnehmer als Auftragsverarbeiter personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieser Vereinbarung zur Auftragsverarbeitung (nachfolgend „Vereinbarung“) oder erhält vom Auftraggeber als Auftragsverarbeiter Zugriff auf solche Daten in Erfüllung seiner Leistungsverpflichtungen.

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der nachfolgenden in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit Leistungen des Auftragnehmers als Auftragsverarbeiter in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder dessen beauftragte Dritte („Unterauftragnehmer“) personenbezogene Daten (nachfolgend „Daten“) des Auftraggebers verarbeiten oder mit diesen in Berührung kommen können.

Die in dieser Vereinbarung verwendeten Begriffe werden entsprechend ihrer Definition in der Verordnung (EU) 2016/679 („DSGVO“) angewendet. Soweit sich aus dieser Vereinbarung oder den anzuwendenden gesetzlichen Vorschriften nicht ausdrücklich etwas anders ergibt, reicht zur Abgabe einer Erklärung in Schriftform ebenfalls die elektronische Form (z. B. E-Mail) aus.

§ 2 Gegenstand und Dauer der Vereinbarung

(1) Diese Vereinbarung regelt die Verpflichtungen der Vertragsparteien nach Art. 28 Abs. 3 DSGVO zum Schutz der personenbezogenen Daten betroffener Personen und ergänzt insoweit den zwischen den Parteien bestehenden Leistungsvertrag.

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

(3) Die Dauer (Laufzeit) der vorliegenden Vereinbarung entspricht der Laufzeit des Leistungsvertrages. Die vorliegende Vereinbarung kann jedoch vom Auftraggeber vorzeitig schriftlich gekündigt werden, sofern der Auftragnehmer im schwerwiegenden Maße gegen diese Vereinbarung bzw. gegen Datenschutzvorschriften verstoßen hat und auch innerhalb einer ihm zur Abhilfe dieses Verstoßes gesetzten Frist keine solche Abhilfe geschaffen hat und dem Auftraggeber eine Fortsetzung der Verarbeitung bis zur vereinbarten Beendigung des Leistungsvertrages nicht zuzumuten ist.

(4) Im Zusammenhang mit dem Leistungsvertrag kann eine Verarbeitung von personenbezogenen Daten als Auftragsverarbeiter im nachfolgend beschriebenen Umfang und Zweck durch den Auftragsverarbeiter erfolgen:

a. Wartung der EDV-Systeme beim Auftraggeber

b. IT-Supportleistungen

c. Websitehosting

d. Software as a Service (SaaS)-Leistungen

e. Dienstleistungen zum Vertrags- und Nachlassmanagement und/oder zur digitalen Formalitätenerledigung

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

§ 3 Konkretisierung der Auftragsverarbeitung

(1) Sofern hierfür der Leistungsvertrag aus Sicht des Auftraggebers nicht ausreichend erscheint, können die Parteien nachfolgend weitere ergänzende Konkretisierungen zur Art und des Zwecks der Verarbeitung vornehmen:

(2) Der Auftragnehmer ist zur Erfüllung des Vertragsgegenstandes aus dem Leistungsvertrag unter Einhaltung der Bestimmungen der vorliegenden Vereinbarung insbesondere zur Durchführung aller erforderlichen Verarbeitungsschritte und Nutzungen der vom Auftraggeber überlassenen oder über ein Dateisystem zugänglich gemachter Daten sowie der ggf. für ihn erhobenen Daten berechtigt. Hierzu gehört neben einer ganz oder teilweise automatisierten Verarbeitung auch die nichtautomatisierte Verarbeitung von Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Verarbeitung kann in diesem Sinne auch das Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files, Zwischendateien und Arbeitsbereichen etc. sein, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

(3) Die betroffenen **Datenarten und -kategorien** (Aufzählung / Beschreibung der Datenkategorien) sind in **Anlage 1** aufgelistet.

§ 4 Ergänzende Verantwortlichkeiten und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten als Auftragsverarbeiter nur im Rahmen der Erfüllung des Leistungsvertrages und im Einklang mit den in dieser Vereinbarung getroffenen sowie den einschlägigen gesetzlichen Bestimmungen. Der Auftragnehmer bestätigt, dass ihm diese Vorschriften bekannt sind, und dass er die in seinem Verantwortungsbereich liegende innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragnehmer unterlässt jedwede Nutzung und Verarbeitung zum privaten, eigenen oder einem anderen gewerblichen oder geschäftlichen Zweck. Er wird den Datenzugriff auf das für die konkrete Auftragserfüllung mögliche Minimum beschränken.

(3) Der Auftragnehmer ist verpflichtet, mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung von Aufträgen betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten, nur im Rahmen der Weisungen des Auftraggebers Daten verarbeiten und die aus dem Bereich des Auftraggebers erlangten Daten nicht an Dritte weitergeben oder sonst abweichend verwerten.

Er gewährleistet, dass alle mit der Verarbeitung betrauten Personen in geeigneter Weise zur Vertraulichkeit verpflichtet wurden, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.

(4) Der Auftragnehmer ergreift alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen. Näheres dazu regelt § 9 der vorliegenden Vereinbarung (Technische und organisatorische Maßnahmen).

(5) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

Hierzu zählen insbesondere das Erstellen und Führen von Verzeichnissen über Verarbeitungstätigkeiten im Auftrag des Auftraggebers nach Art. 30 Abs. 2 DSGVO, als auch notwendige Auskünfte für eine erforderliche Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO. Eine darüberhinausgehende Unterstützung durch den Auftragnehmer, insbesondere eine Unterstützung bei Anfragen der Aufsichtsbehörde an den Auftraggeber in Erfüllung seiner Aufgaben, bedarf einer gesonderten Vereinbarung. Die dem Auftragnehmer dabei entstehenden Aufwände werden von dem Auftraggeber zu den marktüblichen Konditionen erstattet.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

(7) Der Auftragnehmer benennt dem Auftraggeber die/den Datenschutzbeauftragte/n bzw. die verantwortlichen Ansprechpartner für die Datenverarbeitung im Auftrag und Datensicherheit, sowie die jeweiligen weisungsempfangsberechtigten Personen. Die Kontaktdaten dieser Personen sind **Anlage 2** zu entnehmen. Bei Änderung des Datenschutzbeauftragten bzw. der verantwortlichen Ansprechpartner wird der Auftraggeber schriftlich informiert und eine aktualisierte Anlage separat bereitgestellt.

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | www.rapid-data.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

(8) Der Auftragnehmer informiert den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, die Gefahren für die Daten der Auftraggeber mit sich bringen, bei begründetem Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer dem Auftraggeber bei der Einhaltung ihrer Meldepflichten unterstützen. Der Auftragnehmer informiert den Auftraggeber ebenfalls über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung von Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

Die Parteien können sich in einem solchen Falle auf eine Unterbrechung der Verarbeitungstätigkeit einigen, wenn diese nicht aufgrund der jeweiligen Schwere und Tragweite einer Ermittlung/eines möglichen Datenschutzverstoßes ohnehin geboten erscheint. Der Auftragnehmer informiert den Auftraggeber über eine solche Unterbrechung der Verarbeitungstätigkeit. Der Auftragnehmer wird dem Auftraggeber das anschließende Ergebnis einer Überprüfung der Aufsichtsbehörden oder andere zuständigen Behörden im Hinblick auf diese Vereinbarung bekannt geben. Die feststellten Mängel wird der Auftragnehmer unverzüglich bearbeiten und Maßnahmen zum Abstellen dieser Mängel einleiten.

(9) Überlassene Datenträger sowie Daten und sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, den Auftraggeber unaufgefordert zu informieren, soweit seine Daten und Unterlagen von einem unberechtigten Zugriff durch Dritte betroffen sind.

(10) Sollten Daten oder Datenträger des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so wird der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

§ 5 Verarbeitung von personenbezogenen Daten in Privatwohnungen

(1) Der Auftraggeber erlaubt dem Auftragnehmer die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office“) durch seine Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind.

(2) Der Auftragnehmer stellt sicher, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office“ der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer sorgt 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, trägt der Auftragnehmer dafür Sorge, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

§ 6 Verantwortlichkeiten und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, für die Rechtmäßigkeit der Datenverarbeitung, sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | www.rapid-data.de

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Verarbeitungsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt oder sofern er aus irgendwelchen Gründen nicht mehr zur Datenweitergabe an den Auftragnehmer berechtigt ist, ebenso über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde oder der zuständigen Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens, sowie Haftungsansprüchen einer betroffenen Person oder eines Dritten, soweit sie sich auf diese Vereinbarung beziehen oder Auswirkungen auf diese haben können. Hinsichtlich einer Unterbrechung der Datenverarbeitung gelten die in § 4 (8) dieser Vereinbarung niedergelegten Bestimmungen.

(3) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO ist der Auftraggeber verantwortlich, diese eigenverantwortlich abzuwehren. Der Auftragnehmer hat den Auftraggeber hierbei zu unterstützen. § 4 (5) dieser Vereinbarung findet entsprechende Anwendung.

(4) Der Auftraggeber benennt dem Auftragnehmer die/den Datenschutzbeauftragte/n bzw. die verantwortlichen Ansprechpartner für den Datenschutz und für anfallende Datenschutzfragen unter dieser Vereinbarung sowie die jeweiligen weisungsberechtigten Personen. Die Kontaktdaten dieser Personen sind **Anlage 2** zu entnehmen.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

(5) 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.

§ 7 Weisungsbefugnis des Auftraggebers und Weisungsgebundenheit des Auftragnehmers

(1) Entsprechend der in § 4 dieser Vereinbarung niedergelegten Bestimmungen verarbeitet der Auftragnehmer die ihm zur Verfügung gestellten Daten nach den Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Methode der Verbreitungstätigkeiten zu erteilen. Die Weisungsberechtigten sind **Anlage 2** dieser Vereinbarung benannt.

(2) Die Weisungen werden anfänglich durch diese Vereinbarung und den entsprechenden Leistungsvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem vereinbarten elektronischen Format (wie z. B. Ticketsystem, Fax oder E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen oder Aufträge, die in der Vereinbarung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt und bedürfen eine Änderungsvereinbarung in schriftlicher Form. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis deren Rechtmäßigkeit durch den Auftraggeber bestätigt oder in eine rechtlich zulässige Weisung geändert wird.

§ 8 Datenverarbeitung außerhalb der EU/EWR

Die Verarbeitung durch den Auftragnehmer findet nur innerhalb der EU/EWR oder in einem Drittland, bei dem die Verarbeitung durch die Kommission durch einen Angemessenheitsbeschluss nach Art. 45 DSGVO genehmigt wurde, statt. 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. Mit Unterschrift wird die Zustimmung zu den in Anlage 4 aufgeführten Unterauftragsnehmer erteilt.

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

§ 9 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass er den besonderen Anforderungen der einschlägigen Datenschutzbestimmungen gerecht wird und geeignete technische und organisatorische Maßnahmen treffen, welche für die konkrete Verarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau nach dem Stand der Technik gewährleisten und die den Anforderungen des Art. 32 DSGVO genügen.

(2) Der Auftraggeber hat die Möglichkeit, im Rahmen einer Vorabprüfung im Vorfeld der Auftragsvergabe bzw. Verarbeitung die bei dem Auftragnehmer vorhandenen dokumentierten technischen und organisatorischen Maßnahmen vom Auftragnehmer schriftlich anzufordern und einzusehen. Etwaig erforderliche Anpassungen dieser Maßnahmen unter Berücksichtigung des Risikos im Hinblick auf die konkrete Verarbeitungstätigkeit, werden zwischen den Parteien einvernehmlich beschlossen und konkretisiert.

(3) Die konkreten bzw. vereinbarten Maßnahmen sind in **Anlage 3** zu dieser Vereinbarung dokumentiert. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das der Verarbeitung angemessene Schutzniveau nicht unterschritten wird. Soweit nicht abweichend vereinbart, teilt der Auftragnehmer dem Auftraggeber wesentliche Änderungen mit. Die Änderungen werden dem Auftraggeber separat schriftlich übermittelt.

(5) Der Auftragnehmer kontrolliert in regelmäßigen Abständen seine internen Prozesse sowie technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten und Maßnahmen sowie die Aufrechterhaltung der Anforderungen aus dieser Vereinbarung entsprechend den Regeln von § 11 dieser Vereinbarung mit geeigneten Mitteln nach.

§ 10 Rechte Betroffener, Berichtigung, Einschränkung und Löschung von Daten

(1) Die Rechte der durch die Datenerhebung, -verarbeitung und -nutzung beim Auftragnehmer betroffenen Personen sind grundsätzlich gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Er ist dabei insbesondere für die Benachrichtigung der Betroffenen, die Auskunftserteilung an die Betroffenen sowie die Berichtigung, Löschung und Sperrung von Daten verantwortlich. Der Auftraggeber wird den Auftragnehmer unverzüglich über die Berichtung, Löschung oder Sperrung von Daten informieren.

(2) Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und diese Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei Beantwortung und Verfolgung von Anträgen betroffener Personen entsprechend § 4 (5) dieser Vereinbarung. Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer dem Auftraggeber auf dessen Anfrage, die hierfür notwendigen in seiner Sphäre befindlichen Informationen bereitstellen.

(4) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung der Daten und ggf. von Datenträgern und sonstigen Materialien auf Grund einer gesonderten Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Sofern vom Auftraggeber eine Aufbewahrung bzw. Übergabe der Daten angewiesen wird, sind etwaige Schutzmaßnahmen hierzu gesondert zu vereinbaren, sofern nicht in der Vereinbarung bereits vereinbart. Die dem Auftragnehmer entstehenden Aufwände für etwaige Vernichtungen, Aufbewahrungen oder Übergaben der Daten an die betroffene Person werden dem Auftragnehmer vom Auftraggeber erstattet. § 4 (5) dieser Vereinbarung gilt entsprechend.

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

§ 11 Nachweis über Einhaltung von Datenschutzverpflichtungen und Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen durch Kontrollen, Einholung von Auskünften oder Überlassung von entsprechenden Nachweisen durch den Auftragnehmer, zu überzeugen. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Der Nachweis solcher Maßnahmen, die nicht nur die konkrete Vereinbarung betreffen, erfolgt durch, sofern vorhanden:

☒ Durchführung eines Selbstaudits (aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen, z. B. Wirtschaftsprüfer, Datenschutzbeauftragter, Revision, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)

(3) Sollten im Einzelfall Kontrollen durch den Auftraggeber oder einen von diesem beauftragten Prüfer gemäß Art. 28 Abs. 3 lit. h DSGVO vorgenommen werden, können diese von dem betrieblichen Datenschutzbeauftragten des Auftraggebers und den vom Auftraggeber nach **Anlage 2** zu dieser Vereinbarung benannten Personen oder sonstigen vom Auftraggeber beauftragte Personen nach gemeinsamer Abstimmung zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs vorgenommen werden, um sich von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Verarbeitung einschlägigen Datenschutzgesetze zu überzeugen. Bei Bedarf ist dem Auftragnehmer vor der Kontrolle eine von ihm vorbereitete Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden zu unterzeichnen.

(4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten ebenso schriftlich zur Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(5) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Der Aufwand einer Kontrolle ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

§ 12 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen von Unterauftragnehmern (weitere Auftragsverarbeiter) zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung im Rahmen des Leistungsvertrages beziehen. Nicht hierzu gehören Nebenleistungen, beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO in Anspruch zu nehmen. Der Auftragnehmer informiert den Kunden, wenn sie eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 4 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer zu erheben. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunden innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.

(3) Die an der Verarbeitung beteiligten Unterauftragnehmer werden in **Anlage 4** niedergelegt. Bei Änderungen wird die Anlage separat zur Verfügung gestellt, ein Widerruf gegen neue Unterauftragnehmer ist möglich.

(4) Der Auftragnehmer wird mit den in die Verarbeitung eingebundenen Unterauftragnehmern ebenfalls Vereinbarungen treffen und diese so gestalten, dass sie den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragsparteien dieser Vereinbarung entsprechen. Der Auftragnehmer wird die Einhaltung der Pflichten der Unterauftragnehmer in regelmäßigen Abständen kontrollieren und/oder überprüfen.

Der Auftraggeber ist berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | www.rapid-data.de

§ 13 Löschung und Rückgabe von personenbezogenen Daten bei Vertragsbeendigung

(1) Nach Beendigung des Leistungsvertrages oder jederzeit auf Weisung hat der Auftragnehmer die vom Auftraggeber überlassenen Daten, die für den Auftraggeber erhobenen, verarbeiteten und/oder genutzten Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, etwaige Kopien davon sowie in seinen Besitz gelangte Unterlagen dem Auftraggeber auf dessen Anforderung herauszugeben bzw. zurückzugeben. Ist eine Herausgabe bzw. Rückgabe der Daten, sowie etwaiger Kopien der Daten aus technischen Gründen nicht möglich, bspw. infolge elektronischer Speicherung auf fest installierten oder – soweit datenschutzrechtlich zulässig - gemeinsam genutzten Medien oder wird eine Löschung/Vernichtung vom Auftraggeber gewünscht, sind die entsprechenden Daten vom Auftragnehmer in Abstimmung mit dem Auftraggeber datenschutz- konform zu löschen. Gleiches gilt für Test-, Ausschussmaterial und etwaige Datensicherungen. Elektronisch gespeicherte Daten sind auf Wunsch des Auftraggebers entweder in einem marktüblichen Format auf elektronischen Datenträgern herauszugeben oder online zu übertragen. Ausgenommen hiervon sind Sicherungskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(2) Der Auftragnehmer wird die Löschung/Vernichtung dem Auftraggeber schriftlich oder per E-Mail bestätigen. Weitergehende gesetzliche Löschungsverpflichtungen und Löschungsansprüche bleiben von vorstehenden Regelungen unberührt. Zur Löschung/ Vernichtung werden die Standardprozesse des Auftragnehmers genutzt.

§ 14 Vertraulichkeit; Verpflichtung von Mitarbeitern und Dritten

(1) Der Auftragnehmer sichert zu, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und verpflichtet sich zu ihrer Einhaltung. Er verpflichtet sich außerdem, die ihm bei der Ausübung der Aufgaben aus dieser Vereinbarung zur Kenntnis gelangten mündlichen oder schriftlichen Informationen und überlassenen Unterlagen streng vertraulich zu behandeln, es sei denn, er ist durch die geltenden gesetzlichen Bestimmungen zur Veröffentlichung verpflichtet. Er verpflichtet sich, bei Datenverarbeitung die Verschwiegenheit hinsichtlich der Daten zu wahren.

(2) Der Auftragnehmer sichert zu, dass er zur Durchführung dieser Vereinbarung nur Mitarbeiter oder sonstige Dienstleister einsetzt, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Der Auftragnehmer sichert ferner zu, dass er zur Durchführung dieser Vereinbarung nur Mitarbeiter oder sonstige für ihn tätige Dienstleister einsetzt, denen es untersagt ist, die Daten außerhalb der vertraglichen Vereinbarung oder dokumentierter Weisungen zu verarbeiten.

(4) Die Verpflichtung nach Absatz (1) bis (2) gelten auch nach Beendigung dieser Vereinbarung fort.

§ 15 Haftung

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 so lange 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.

§ 16 Vergütung

Vereinbarungen zur Vergütung sind im Leistungsvertrag geregelt.

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | www.rapid-data.de

§ 17 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen der Schriftform, sofern nicht ausdrücklich anders vereinbart. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Nebenabreden sind nicht getroffen.

(2) Die Vertragsbegründung, Vertragsänderungen und (mündliche) Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Mitteilungen/Informationen, Zustimmungen, Genehmigungen und Bestätigungen können per E-Mail erfolgen.

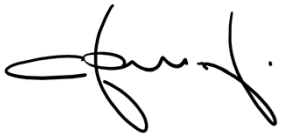
(3) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt. Die Parteien treffen eine entsprechende Bestimmung, die dieses Ziel erfüllt.

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

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

§ 18 Unterschriften

_____	_____
Ort, Datum	(Auftraggeber)
Berlin, 02.04.2025	
_____	_____
Ort, Datum	(Auftragnehmer) Christian Lang Geschäftsführer Rapid Data GmbH Unternehmensberatung

Rapid Data GmbH Unternehmensberatung | Ritterstraße 3 | 10969 Berlin | Tel. +49 30 208 98 17-40 | Fax +49 30 208 98 17-49
Standort Selmsdorf: An der Trave 7a | 23923 Selmsdorf | Tel. +49 451 619 66-0 | Fax +49 451 619 66-99
Sitz der Gesellschaft: Berlin | Geschäftsführer: Christian Lang, Markus Kreitinger | Amtsgericht Berlin-Charlottenburg
HRB 236811 B | USt.-ID: DE283664602 | info@rapid-data.de | **www.rapid-data.de**

Anlage 1 – Beschreibung erhobenen Datenarten und Datenkategorien

Folgende betroffene **Datenarten und -kategorien** werden verarbeitet**:**

- Name
- Vorname
- Geburtsdatum
- Adresse
- Telefonnummer
- E-Mailadresse
- Vertragliche Beziehung - Kundenkontoinformationen
- Personenstammdaten / pers. Identifikationsdaten (z. B. Name, Anschrift, Geburtsdatum, Familienstand, Berufsbezeichnung, Firmenzugehörigkeit, Online-Kennung)
- Elektronische Identifikationsdaten (wie IP-Adresse, Elektronische Unterschrift, Verbindungs-/Protokolldaten, Cookies) von Mitarbeitern verbundener Unternehmen
- Sozialdaten (d.h. alle Daten, die bspw. von Sozialleistungsträgern sowie deren Verbänden und Arbeitsgemeinschaften verarbeitet werden)
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten (Bank, Kontoverbindung, Kreditkartendaten)

Sofern personenbezogene Daten nach Artikel 9 DSGVO erhoben werden, können diese umfassen:

- Gewerkschaftszugehörigkeit

  (Sofern Kunden des Auftraggebers Vorsorge-Dienstleistungen nutzt)
- Religiöse Überzeugung, Sexualleben oder sexuelle Orientierung
  (Sofern Kunden des Auftraggebers Vorsorge-Dienstleistungen
  nutzt)

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden des Auftraggebers
- Interessenten
- Angehörige
- Mitarbeiter des Auftraggebers

Anlage 2 - Kontaktdaten und Zuständigkeiten und zu nutzende Kommunikationskanäle

1) Berechtigte Personen

Die nach § 7 Abs. (1) der Vereinbarung zur Weisung berechtigten Personen **beim Auftraggeber** sind:

Name	Vorname	Titel/Funktion	Anschrift	Telefon	E-Mail

2) Meldung datenschutzrelevanter Vorfälle

Datenschutzrelevante Vorfälle gemäß § 7 Abs. (3) der Vereinbarung sind unmittelbar nach ihrer Feststellung und ohne schuldhafte Verzögerung vom Auftragnehmer an den Auftraggeber zu melden. Hierfür sind **auf Seiten des Auftraggebers** die folgenden Personen **innerhalb der üblichen Geschäftszeiten** zu informieren:

Name	Vorname	Titel/Funktion	Anschrift	Telefon	E-Mail

3) Für Weisungen zu nutzende Kommunikationskanäle:

Weisungsempfänger beim Auftragsverarbeiter sind: Der jeweilige für den konkreten Auftrag verantwortliche Mitarbeiter des Auftragsverarbeiters: Per E-Mail an die persönliche Mailadresse des Ansprechpartners oder an support@rapid-data.de.

4) Ansprechpartner beim Auftragnehmer

Als Ansprechpartner bezüglich des Datenschutzes auf **Seiten des Auftragnehmers** stehen die folgenden Personen zur Verfügung:

Name	Vorname	Titel/Funktion	Anschrift	E-Mail
Christian	Lang	Geschäftsführer	Ritterstraße 3, 10969 Berlin	support@rapid-data.de
Dennis	Schulz	Datenschutzbeauftragter	LOROP GmbH, Landgrafenstraße 16, 10787 Berlin	datenschutz@lorop.de

Anlage 3 – Beschreibung der technischen und organisatorischen Maßnahmen des Dienstleisters

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem solche, die zur Zutritts-, Zugriffs-, oder Zugangskontrolle gehören. In diesem Zusammenhang sollen die folgenden technischen und organisatorischen Maßnahmen des Auftragnehmers eine angemessene Sicherheit von personenbezogenen Daten gewährleisten, einschließlich des Schutzes von unbefugter oder unrechtgemäßer Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

a) Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Folgende Maßnahmen sind beim Auftragnehmer umgesetzt:

☐	Absicherung von Gebäudeschächten	☐	Protokollierung der Besucher
☐	Alarmanlage	☒	Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe
☐	Automatisches Zutrittskontrollsystem	☒	Schlüsselregelung (Schlüsselliste)
☐	Biometrische Zutrittskontrollen	☐	Sicherheitstüren und -schlösser
☒	Chipkarten-/Transponder-Schließsystem	☒	Anweisung zur Ausgabe von Schlüsseln
☐	Einbruchmeldeanlage	☐	Sorgfältige Auswahl von Wachpersonal
☐	Einsatz von Wachpersonal	☐	Tragepflicht von Berechtigungsausweisen
☐	Lichtschranken / Bewegungsmelder	☐	Unterteilung in verschiedene Sicherheitszonen
☒	Manuelles Schließsystem	☐	Videoüberwachung der Zugänge
☐	Personenkontrolle beim Pförtner / Empfang	☐	Zutrittsberechtigungen funktions- und rollenbasiert
☐	sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. Die Überwachung des Geländes/Gebäudes erfolgt außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen durch einen externen Wachdienst.		

b) Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☐	2-Faktor-Authentifizierung	☒	Passwortregelung (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperrung/Löschung u.a.)
☒	Authentifikation mit Benutzername / Passwort	☒	Schlüsselregelung (Schlüsselausgabe etc.)
☐	Authentifikation mit biometrischen Verfahren	☐	Sichere Aufbewahrung von Datenträgern (Sicherungsbänder, Festplatten etc.)

☐	Einsatz eines Aktenvernichters	☐	Sorgfältige Auswahl von Transportpersonal und -fahrzeugen*
☒	Einsatz von Anti-Viren-Software	☐	Vernichtung von Datenträgern durch dafür zertifizierte Entsorgungsfachbetriebe
☒	Einsatz einer Hardware-Firewall	☒	Vernichtung von Papierdokumenten durch dafür zertifizierte Entsorgungsfachbetriebe -
☐	Einsatz eines Identity Management Systems	☐	Notfallmanagement für Auftraggeber (u.a. Mehrschichtbetrieb, Rufbereitschaft, Stellvertreterregelung) *
☐	Einsatz einer Software-Firewall	☒	Zuweisung von Benutzerrechten erfolgt funktions- und rollenbasiert.
☒	Einsatz verschließbarer Entsorgungsbehälter für Papier, Akten und Datenträger	☒	Netzwerk- und Netzwerkzonenkonzept
☒	Einsatz von VPN-Technologie*	☒	Zuordnung von Benutzerprofilen zu IT-Systemen
☒	Erstellen von Benutzerprofilen	☐	Verwendung sicherer Transportbehälter /-verpackungen beim physischen Transport*
☐	sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. Die mit * gekennzeichneten Maßnahmen bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.		

c) Zugriffskontrolle/Speicherkontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☒	Anzahl der Administratoren auf ein Minimum begrenzt	☐	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten*
☒	Funktions- und rollenbasiertes Berechtigungskonzept	☐	Verwaltung der Zugriffsberechtigungen unter Beachtung der Funktionstrennung und des 4-Augenprinzip
☐	Protokollierung der Vernichtung von Papier, Akten und Datenträgern		

d) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	☐	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒	Festlegung von Datenbankrechten	☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern
☐	Logische Mandantentrennung (softwareseitig)	☒	Trennung von Produktiv- und Testsystem*

☐	sonstiges: siehe 5. Eingabekontrolle. Wurde mit dem Auftraggeber nicht anderes vereinbart, erfolgt die Datenverarbeitung logisch getrennt. Die mit * gekennzeichneten Maßnahmen bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.

e) Pseudonymisierung

Pseudonymisierung ist 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 entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Maßnahmen im Zusammenhang mit der Pseudonymisierung personenbezogener Daten sind nach Weisung des Auftraggebers:

☐ Auswahl eines geeigneten Verfahrens zur Pseudonymisierung nach dem aktuellen Stand der Technik*	☐ Pseudonymisierung von Daten nach einem risikobasierten Ansatz entsprechend den unterschiedlichen Schutzbedarfskategorien von Daten*
☐ Pseudonymisierungsgebot ist zentraler Bestandteil im Rahmen des Datenschutzkonzepts des Auftragnehmers	☐ Einsatz von Software, die Management pseudonymisierter Daten erlaubt*
☐ Gesicherte Aufbewahrung der zur Pseudonymisierung verwendeten kryptographischen Schlüssel bzw. Kontrolllisten (ggf. verschlüsselte Speicherung von Kontrolllisten) *	☐ Berechtigungskonzept für den Zugriff auf kryptographische Schlüssel bzw. Kontrolllisten, die eine Personalisierung ermöglichen*
☒ sonstiges: Die Pseudonymisierung von Daten des Auftraggebers erfolgt nur nach Weisung und nur in Abstimmung mit dem Auftraggeber. Die mit * gekennzeichneten Maßnahmen bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.	

f) Verschlüsselung

Durch Verschlüsselung soll die Kenntnisnahme in personenbezogene Daten durch Unbefugte geschützt oder diese zur Kenntnis genommen werden (z. B. durch Hackerangriffe oder Spionage). Verschlüsselung bezeichnet die Umwandlung von Daten in eine Form, die man als Chiffretext bezeichnet und die von nicht autorisierten Personen kaum zu verstehen ist.

Maßnahmen im Zusammenhang mit der Verschlüsselung personenbezogener Daten sind nach Weisung des Auftraggebers:

☒ Auswahl eines geeigneten kryptographischen Verfahrens nach dem aktuellen Stand der Technik*	☐ Regelmäßige Überprüfung von eingesetzten Verschlüsselungsverfahren auf Sicherheitslücken und ggf. die erforderliche Aktualisierung der dafür eingesetzten Software*
☒ E-Mail-Verschlüsselung*	☐ Verschlüsselungsrichtlinien berücksichtigen die unterschiedlichen Schutzkategorien personenbezogener Daten*
☐ Einsatz von Verschlüsselungsverfahren entsprechend Datenschutzkonzept*	☐ Löschungskonzept für versendete verschlüsselte Dateien*

☐ Prozesse zur Verwaltung und zum Schutz der kryptographischen Informationen (Berechtigungskonzept für interne und externe Mitarbeiter) *	☐ Verschlüsselung auf Verzeichnis- und Dateiebene*
☐ Verschlüsselung von mobilen Datenträgern (USB-Sticks, CD/DVD etc.) *	☒ Verschlüsselung von Datenträgern in Laptops / Notebooks ☐ Verschlüsselung von Smartphone Inhalten
☐ sonstiges: Die Verschlüsselung von Daten des Auftraggebers erfolgt nur nach Weisung und nur in Abstimmung mit dem Auftraggeber. Die mit * gekennzeichneten Maßnahmen bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.	

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen zur Umsetzung des Gebots der Integrität sind zum einen solche, die auch zur Eingabekontrolle gehören, zum anderen aber auch solche, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen. In diesem Zusammenhang sollen die folgenden technischen und organisatorischen Maßnahmen des Auftragnehmers die Integrität von personenbezogenen Daten gewährleisten.

a) Datenträgerkontrolle/ Übertragungskontrolle/Transportkontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen*	☒	Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis gem. § 88 TKG
☒	E-Mail-Verschlüsselung*	☐	Verpflichtung der Mitarbeiter auf das Sozialgeheimnis ge. §35 SGB I
☒	Einrichtung von Standleitungen bzw. VPN-Tunneln*	☒	Verpflichtung der Mitarbeiter auf das Verbot des Verrats von Geschäfts- und Betriebsgeheimnissen gem. §§ 17 ff. UWG
☐	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen*	☒	Verpflichtung der Mitarbeiter auf Zweckbindung und Geheimhaltungspflicht gem. § 78 Abs. 1 SGB X
☒	Verpflichtung der Mitarbeiter auf das Datengeheimnis	☐	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form*
☒	sonstiges: Die Weitergabe von Daten des Auftraggebers erfolgt nur in Abstimmung mit dem Auftraggeber and die von ihm vorgegebenen Empfänger. Alle Mitarbeiter des Auftragnehmers sind zur Wahrung der Verschwiegenheit sowie des Datengeheimnisses als Bestandteil ihres Arbeitsvertrages mit dem Auftragnehmer verpflichtet und über die rechtlichen Konsequenzen im Fall der Zuwiderhandlung schriftlich belehrt. Die mit * gekennzeichneten Maßnahmen bedürfen einer individuellen, schriftlichen Beauftragung durch den Auftraggeber.		

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☒	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind	☐	Protokollierung der Eingabe, Änderung und Löschung von Daten
☐	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können	☐	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeots
☐	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)		

3. Verfügbarkeit und Belastbarkeit von Systemen (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, welche gewährleisten, dass Daten und IT-Systeme zur Verfügung stehen und von autorisierten Personen genutzt werden können, wenn dies benötigt wird. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar. Ebenfalls sind dies Maßnahmen, durch welche sichergestellt wird, dass Systeme auf denen personenbezogene Daten gespeichert sind einer gewissen Beanspruchung standhalten können, regelmäßig überwacht werden und für die ein entsprechendes Notfallmanagement etabliert wurde.

a) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind. Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

☐	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☐	Notfallhandbuch
☐	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☐	Notfallkonzept (BCM)
☐	Feuer- und Rauchmeldeanlagen	☐	Notfallplan
☐	Feuerlöschanlagen in Serverräumen	☐	Regelungen zur Verfügbarkeit und Zuverlässigkeit der vom Auftragnehmer erbrachten Leistung
☐	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Überspannungsschutzkonzept in Serverräumen
☒	Klimatisierte Serverräume	☐	Maßnahmen gegen Wassereinbruch in Serverräume
☒	Konzept zur Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery) durch den Auftragnehmer	☐	Testen von Datenwiederherstellung
☐	Konzept zur Archivierung von Daten durch den Auftragnehmer	☒	Unterbrechungsfreie Stromversorgung (USV)

b) Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer

Hierzu gehören Maßnahmen, die vom Auftragnehmer eingesetzt werden, um eine Überwachung der Systeme und eine mögliche Belastung von Systemen frühzeitig zu erkennen und zu vermeiden.

☐	Load-Balancing	☒	Dynamische Prozesse und Speicherzuschaltung
☐	Penetrationstests	☒	Belastungstests der Datenverarbeitungssysteme
☐	Belastungsgrenze für das jeweilige System im Voraus über das notwendige Minimum ansetzen*	☐	Details siehe 3 a) „Verfügbarkeitskontrolle“

c) Wiederherstellbarkeit

Zur Sicherstellung einer Fähigkeit auf Wiederherstellung können Maßnahmen zur regelmäßigen Sicherung der Systeme eingesetzt werden wie auch entsprechende Maßnahmenpläne, die Einführung und Aufrechterhaltung eines Notfallmanagements inkl. Notfallpläne oder entsprechenden Leitfäden sowie regelmäßige Tests.

Details siehe 3 a) „Verfügbarkeitskontrolle“

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Organisationskontrolle

Maßnahmen zur Gestaltung der innerbetrieblichen Organisation, die den besonderen Anforderungen des Datenschutzes gerecht werden.

☒	Datenschutz-Management	☐	Tätigkeiten der Mitarbeiter in Stellen-, Funktions- und Rollenbeschreibungen
☐	Benachrichtigungsverfahren	☒	Incident-Response-Management
☐	Auskunftsverfahren	☐	Entsorgungskonzept
☐	Trennung der Funktionen und Verantwortung zwischen Dateneigentümer und Datenverarbeiter	☒	Schulung der Mitarbeiter im Umgang mit dem Datenschutzgesetz
☒	Bestellung eines Datenschutzbeauftragten; festlegen und bekanntgeben seiner Aufgaben	☒	Datensicherheitslinie
☒	Erstellung und Pflege eines Verzeichnisses der Verarbeitungstätigkeiten für Auftragsverarbeiter	☐	Richtlinie zu einzusetzender Hard- und Software einschließlich Investitions- und Genehmigungsverfahren
☐	Katastrophenrichtlinie zur schnellen Wiederinbetriebnahme der Datenverarbeitungsanlagen		
☐	sonstiges: Einzelheiten zur auftrags- und verarbeitungsspezifischen Organisationskontrolle sind in § 3 ff. der hier vorliegenden Vereinbarung beschrieben.		

b) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Folgende Maßnahmen werden zusätzlich zu den vorgenannten Kontrollen vom Auftraggeber und vom Auftragnehmer umgesetzt:

Maßnahmen, die die <u>Auftragsverarbeitung durch den Auftragnehmer</u> regulieren:		Maßnahmen, die eine mögliche Auftragsdatenverarbeitung durch den Unterauftragnehmer des Auftragnehmers regulieren:	
☒	Auswahl des Auftragnehmers durch den Auftraggeber unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	☐	Auswahl des Unterauftragnehmers durch den Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
☒	Prüfung des Auftraggebers auf Bestellung eines Datenschutzbeauftragten beim Auftragnehmer	☐	Prüfung des Auftragnehmers auf Bestellung eines Datenschutzbeauftragten beim Unterauftragnehmer
☒	Prüfung der Dokumentation und der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen durch den Auftraggeber vor Beginn der Datenverarbeitung	☒	Prüfung der Dokumentation und der beim Unterauftragnehmer getroffenen Sicherheitsmaßnahmen durch den Auftragnehmer vor Beginn der Datenverarbeitung
☒	Schriftliche Weisungen des Auftraggebers an den Auftragnehmer (z.B. durch Vereinbarung der Datenverarbeitung im Auftrag)	☒	Schriftliche Weisungen des Auftragnehmers an den Unternauftragnehmer (z.B. durch Vereinbarung der Datenverarbeitung im Auftrag)
☐	Vertragsstrafen bei Verstößen mit dem Auftragnehmer vereinbart	☐	Vertragsstrafen bei Verstößen mit dem Unterauftragnehmer vereinbart
☒	Wirksame Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer vereinbart	☐	Wirksame Kontrollrechte des Auftragnehmers gegenüber dem Unterauftragnehmer vereinbart
☐	Sicherstellung der Vernichtung von Daten durch Auftraggeber und Auftragnehmer nach Beendigung des Auftrags	☐	Sicherstellung der Vernichtung von Daten durch den Auftragnehmer und Unterauftragnehmer nach Beendigung des Auftrags gemä0 schriftlicher Weisung des Auftraggebers
☐	Vertragliche Vereinbarung zwischen Auftraggeber und Auftragnehmer zum Einsatz von Unterauftragnehmern beim Auftragnehmer		
☐	sonstiges: Weitere Maßnahmen zur Auftragskontrolle siehe Eingabekontrolle. Soweit zwischen Auftraggeber und Auftragnehmer vertraglich nicht anders vereinbart, bedarf der Einsatz von Unterauftragnehmern zur Ausführung der vom Auftraggeber an den Auftragnehmer übergebenen Arbeiten, der schriftlichen Zustimmung des Auftraggebers. Es wird auf den dieser Vereinbarung zugrundeliegenden Dienstleistungsvertrag zwischen Auftraggeber und Auftragnehmer verwiesen.		

Anlage 4 - Aufstellung der Unterauftragnehmer i. S. d. § 12 dieser Vereinbarung

Zum Zweck der Erfüllung des Leistungsvertrages setzt der Auftragnehmer die folgenden Unterauftragnehmer ein, deren Einsatz der Auftraggeber hiermit zustimmt, sofern nicht bereits über den Leistungsvertrag geschehen. Soweit zwischen Auftraggeber und Auftragnehmer vertraglich nicht anders vereinbart, ist jede Erweiterung der hier dokumentierten Unterauftragsverhältnisse dem Auftraggeber vom Auftragnehmer mitzuteilen.

Unterauftragnehmer (Firmenname)	**Unterauftragnehmer (Adresse)**	**Zweck**	**Sitz (innerhalb EU / EWR /Angemessenheitsbeschluss)**	**Garantien / Vereinbarungen**
Salesforce.com EMEA Limited	Village 9, Floor 26 Salesforce Tower, 110 Bishopsgate, London, UK	Dienstleistungen; Lizenzverwaltung; Beratung, Entwicklung und Applikations- Management; E-Mail-Services;	Ja	Vertrag zur Auftragsdatenvereinbarung gem. Art. 28 DSGVO Das Vereinigte Königreich ist sicheres Drittland
Microsoft Ireland Operations Limited	South County Business Park, One Microsoft Court, Carmanhall and Leopardstown, Dublin, D18 DH6K, Irland	Hosting Dienstleistungen	Ja	Regelung durch die Bestimmungen für Onlinedienste
Host Europe GmbH	Hansestraße 111, 51149 Köln	Hosting, Dienstleistungen	Ja	Vertrag zur Auftragsdatenvereinbarung gem. Art. 28 DSGVO
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen	Fernwartung Dienstleistungen	Ja	Vertrag zur Auftragsdatenvereinbarung gem. Art. 28 DSGVO
documentus GmbH Berlin & Co. Betriebs KG	Kanalstraße 30 12357 Berlin	Dienstleistungen für Aktenvernichtung	Ja	Datenträgervernichtungsvertrag
Marli GmbH	Carl-Gauß-Straße 13-15, 23562 Lübeck	Dienstleistungen für Aktenvernichtung	Ja	Datenträgervernichtungsvertrag