Vertrag über die Verarbeitung von Daten im Auftrag
(Anlage zum Dienstleistungsvertrag)

1. Allgemeines

(1) Diese Auftragsverarbeitungsvereinbarung ist integraler Bestandteil des zwischen den Parteien geschlossenen Dienstleistungsvertrags („Hauptvertrag“) und gilt automatisch mit Unterzeichnung des Hauptvertrags.

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

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

2. Gegenstand des Auftrags

Der Gegenstand 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 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 3 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den

Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

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

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.
(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

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

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der

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

7. Mitwirkungspflichten des Auftragnehmers

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

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

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

8. Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen 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 trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.

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

(5) Sofern auch bei Unterauftragnehmern Beschäftigte an mobilen Arbeitsplätzen eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. Kontrollbefugnisse

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

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

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. 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 3 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 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der Anlage 2 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 DSGVO 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 2 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 Datenschutzbeauftragten gemäß Art. 37 DSGVO 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 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(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 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(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.

12. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu 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 DSGVO nachkommen kann. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Ausübung der ihr nach den Art. 15 ff. DSGVO zukommenden Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Kunden weiterleiten.

(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.

13. Geheimhaltungspflichten

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

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

14. Vergütung

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

15. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 zu diesem Vertrag beigefügt. Die Parteien sind sich

darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

16. Dauer des Auftrags

(1) Diese Vereinbarung tritt automatisch mit Abschluss des Hauptvertrags in Kraft und gilt für dessen gesamte Laufzeit.

(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.

17. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Erfolgt innerhalb von drei Monaten nach Vertragsende keine Weisung des Auftraggebers, werden die Daten spätestens dann gelöscht. Die Löschung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

18. 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.

(4) Als Gerichtsstand wird das für den Auftragsverarbeiter örtlich zuständige Gericht vereinbart.

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

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

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Gegenstand des Auftrags ergibt sich im Wesentlichen aus dem Hauptvertrag, weshalb im Folgenden nur eine kurze Auflistung erfolgt:

Der Auftrag umfasst folgende Leistungen:

- Administrative Wartung und Betreuung der beim Auftraggeber installierten IT-Infrastruktur.
- Wartung oder Support eines Datenverarbeitungsverfahrens mit der Möglichkeit des Zugriffs auf personenbezogene Daten.
- Operative Verarbeitung personenbezogener Daten im Rahmen der Leistungserbringung.
- Entwicklung individueller Softwarelösungen und Beratung zum Aufsatz und Betrieb der Software COMAN.

Der Zweck der Verarbeitung besteht darin, den sicheren, stabilen und effizienten Betrieb der beim Auftraggeber installierten IT-Infrastruktur und der genutzten Datenverarbeitungsverfahren zu gewährleisten.

Der Auftragnehmer darf Auftraggeber Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen, insbesondere für statistische Zwecke.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind Gegenstand dieses Auftrags:

- Name, Vorname
- Telefonnummer
- E-Mail-Adresse
- Technische Daten der Endgeräte [Betriebssystem, OS-Version, ...]
- Verbindungsinformationen [IP-Adresse, MAC-Adresse, ...]
- Support- und Servicedaten [Korrespondenz, Verbindungszeitpunkt und –dauer)
- Besondere Kategorien personenbezogener Daten (bspw. Gesundheitsdaten, Daten über die rassische / ethnische Herkunft) werden im Rahmen des Auftragsverarbeitungsverhältnisses nicht verarbeitet.

3. Kategorien betroffener Person

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- Mitarbeiter des Auftraggebers/des Verantwortlichen
- Dienstleister des Auftraggebers/des Verantwortlichen
- Andere Personen denen der Auftraggber / der Verantwortliche Zugriff erteilt

Anlage 2 - Unterauftragnehmer

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

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Subunternehmer	**Adresse**	**Gegenstand der Beauftragung**	**Datenübermittlung in Drittstaaten (Rechtsgrundlage)**
Cronon GmbH[1]	Otto-Ostrowski-Straße 7, 10249 Berlin, Deutschland	Rechenzentrum	n/a
Atlassian Pty Ltd	Level 6, 341 George Street, Sydney NSW 2000, Australien	Ticketsystem	Angemessenheitsbeschluss der EU-Kommission nach Art. 45 (EU-US Data Privacy Framework zertifziert) und Standardvertragsklauseln
HubSpot, Inc.	2 Canal Park, Cambridge, MA 02141, USA	CRM und Websitehosting	Angemessenheitsbeschluss der EU-Kommission nach Art. 45 (EU-US Data Privacy Framework zertifziert) und Standardvertragsklauseln
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	Remotezugriff	n/a
sipgate GmbH	Gladbacher Straße 74, 40219 Düsseldorf, Deutschland	Cloud-Telefonanlage	n/a

1 Dieser Unterauftragnehmer wird nur dann Bestandteil dieses Auftragsverarbeitungsvertrages, sofern und soweit das betreffende Produkt als On-Premise-Installation betrieben wird. Bei Nutzung der SaaS-Lösung des Auftragnehmers entfällt dieser Unterauftragnehmer.

Microsoft Ireland Operations Ltd[2]	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Cloud-Infrastruktur/Hosting (Azure)	Hosting in der EU. Im Falle möglicher Zugriffe/Übermittlungen in Drittstaaten (insb. USA) im Rahmen von Support-/Wartungsleistungen; EU-U.S. Data Privacy Framework (DPF) und/oder EU-Standardvertragsklauseln

2Dieser Unterauftragnehmer wird nur dann Bestandteil dieses Auftragsverarbeitungsvertrages, sofern und soweit das betreffende Produkt als SaaS-Lösung des Auftragnehmers genutzt wird. Bei On-Premise-Installation entfällt dieser Unterauftragnehmer.

Anlage 3

Technische und organisatorische Maßnahmen des Auftragnehmers

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

Transparenz

- Dokumentation erforderlicher Datenschutzfolgeabschätzungen (DSFA)
- Einwilligungserklärung zu Bild-, Ton- und Videoaufnahmen (Aufzeichnung Web-/Videokonferenz)
- Die Datenempfänger der Verarbeitungstätigkeiten sind gesetzeskonform dokumentiert
- Die Art, der Umfangs, die Umstände und die Zwecke der Verarbeitung sind gesetzeskonform nach Art. 30 DSGVO dokumentiert
- Sorgfältige Auswahl des Auftragnehmers (Auftragskontrolle / Sicherheit der Verarbeitung)
- Erlaubnisbasiertes Verfahren – Double-Opt-In-Verfahren (DOI)
- Prozess für auskunftsersuchenden Betroffenen
- Dokumentation verbindlicher Löschfristen
- Signal-Hinweis und Funktionsbeschreibung für Anlagen und Anwendungen zur Aufschaltung auf laufende Gespräche (Mithören) – Telefonanlagen (TK-Anlage)
- Dokumentation von Auftrags- und Unterauftragsverhältnissen

Zweckbindung

- Entgegennehmen von Weisungen nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers
- Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DSGVO
- Im Verzeichnis der Verarbeitungstätigkeiten ist der Zweck der Verarbeitung korrekt gepflegt

Datenminimierung

- Video Hosting auf der eigenen Website – Einbindung eigener Videos
- Datenschutz wird durch datenschutzfreundliche Gestaltung der Technik (Privacy-by-Design) von Produkten und Leistungen umgesetzt
- Festlegung verbindlicher Löschfristen (Löschkonzept)
- Regelmäßige Audits über den Umfang der verarbeiteten Daten durch den Datenschutzbeauftragten

Richtigkeit

- Captcha-Dienst / Spam-Prävention für Websites
- Personen werden bei Anfragen zu personenbezogenen Daten korrekt identifiziert
- Dokumentation zum Nachweis der Datenherkunft
- Es besteht ein geregelter Prozess zur zentralen Verwaltung (Änderung) von Benutzeridentitäten (Benutzerkennung)
- Unverzügliche Löschung unrichtiger und nicht korrigierbarer Daten

Vertraulichkeit - Zutrittskontrolle

- Protokollierung und Auswertung der Zugangskontrolle
- Physisches Schließsystem (Sicherheitsschlösser)
- Wachpersonal (Patrouille)
- Diebstahl- und Einbruchsschutz für Räume der technischen Infrastruktur

- Einbruchmelder - Zutrittskontrolle
- Zutrittskontrolle zu Servern (Räumliche Gegebenheiten Büro, Kanzlei, Praxis)
- Einsatz eines Intrusion-Prevention-Systems
- Nutzung von Blickschutzfiltern bei mobilen Geräten in öffentlichen Räumen (Personennahverkehr, Hotels, Restaurants)
- Netzwerk mit demilitarisierter Zone (DMZ)
- Elektronisches Schließsystem (Sicherheitsschlösser mit Codesperren)
- Es sind Sicherheitsüberwachungssystem in den Bereichen vorhanden, in denen personenbezogene Daten verarbeitet werden
- Führen eines Schlüsselbuchs (Dokumentation der Zutrittskontrolle)
- Jeder Nutzer der IT verfügt über eine individuelle Benutzerkennung
- Umsetzung von Sicherheitszonen und klaren Zutrittsbefugnissen
- Auswahl von Reinigungs- und Wachpersonal und Verpflichtung zur Vertraulichkeit und Verschwiegenheit
- Datenverarbeitungsanlagen (z. B. Server) sind sicher im Sicherheitskäfig bzw. Sicherheitsschrank verwahrt
- Die Abmeldung von Systemen (z. B. Windows oder Websoftware) von Nutzern erfolgt automatisch nach einem definierten Zeitraum (Time-Out) bzw. der Zugriff auf den Computer wird durch Sperrung beschränkt.
- Besuchermanagement (Anmeldung/ Empfang/Begleitung)
- Zutrittskontrolle zu Räumen der Datenverarbeitung
- Videoaufzeichnungen definierter Bereich
- Reinigungszeiten während der Arbeitszeit unter Aufsicht
- Sicherung des Raumes der Datenverarbeitungsanlagen
- Regelung zur Sperrung von Zugängen ausscheidender Mitarbeiter (Offboarding)
- Besuchermanagement (Anmeldung/ Empfang/Begleitung)

Vertraulichkeit - Zugangskontrolle

- Umsetzung von Rollen- und Rechtemanagement (Rollen- und Berechtigungskonzept)
- Home-Office / Telearbeit: Vertraulichkeit bei Telefon- und Videokonferenzen
- Benutzer (sind angewiesen) den Computer beim Verlassen des Arbeitsplatzes zu sperren (Bildschirmsperre)
- Nutzung sicherer Datenübermittlungsverfahren, die eine Manipulation versendeter Daten verhindern (z.B. DE-Mail, VPN, verschlüsselte Mails, verschlüsselte Dateien)
- Verfahren zur Authentifizierung–Authentifikation mittels Passworteingabe oder biometrischer Scans
- Firewall-Lösung als Cloud-Service (Einsatz Security-Stack)
- Der Zugriff auf Verzeichnisdienste (z. B. Dateien auf einem gemeinsamen Server) ist durch Authentifizierungsmaßnahmen (Username + Passwort) beschränkt.
- Einsatz einer Firewall zum Schutz des internen Netzwerkes
- Regelung zur Einrichtung von Zugängen neuer Mitarbeiter in die digitalen Systeme des Unternehmens (Onboarding-Prozess)
- Zugangskontrollsystem (ZKS)
- Benutzer (sind angewiesen) den Computer beim Verlassen des Arbeitsplatzes zu sperren (Bildschirmsperre)
- Passwortrichtlinie (Kennwortrichtlinie)
- Zwei-Faktor-Authentisierung (2FA) wird wenn möglich zum Login angewendet

Vertraulichkeit - Zugriffskontrolle

- Managed Print Services (MPS)/Geräte- und Dokumentenmanagement (Monitoring)
- Administratorrechte sind auf verschiedene Personen aufgeteilt, Super-Administratoren werden möglichst vermieden
- Home-Office / Telearbeit: Gewährleistung der Dokumentensicherheit / Lagerung und Verschluss von Papierunterlagen
- Verpflichtung zur Wahrung des Datengeheimnisses und Verschwiegenheitserklärung
- Minimierung von Administratorzugängen
- Mobile-Device-Management im Einsatz
- Trennung von Test- und Produktivsystemen
- Home-Office / Telearbeit: Umgang mit Papierdokumenten (Risiken der Schädigung)
- Delegation von Benutzerrechten und Programmberechtigungen – Rollen- und Rechtemanagement
- Einsatz von Dateiverschlüsselung
- Die sichere Vernichtung personenbezogener Daten in Papierform ist gewährleistet.
- Protokollierung von Anmeldevorgängen
- Verwendung privater Hardware (BYOD)
- Zugriffskontrolle zur Benutzung eines Datenverarbeitungssystems
- Sichere Internetverbindung/Verschlüsselung im Internet (SSL, TLS)
- Verschlüsselte Nutzung eines WLAN für Bürotätigkeiten
- Ein Plan zum Patch Management ist vorhanden und ist fester Bestandteil der IT-Organisation.
- Einsatz von Datenträgerverschlüsselung
- Identitätsmanagement (IdM) und Identity and Access Management (IAM oder IdAM)
- Einsatz von Mailverschlüsselung
- Einsatz von VPN-Netzwerk
- Deaktivierung nicht benötigter Netzwerk-Ports (Netzwerksicherheit / Serversicherheit)
- Enterprise Mobility Management (EMM)
- Aufbewahrung mobiler Speichermedien bei Nichtgebrauch
- Schutz von Betriebs- und Geschäftsgeheimnissen
- Datenklassifizierung

Integrität

- Kabelgebundener Netzwerkzugang: Network Admission Control
- Einsatz von Betriebssystemen und Sicherheits-Updates
- Schutzmaßnahmen zur sicheren Nutzung von E-Mail-Diensten (E-Mail-Sicherheit bei Spam, Malware und Phishing)
- Auswahl und Einsatz von (Standard-)Software
- Barrierefreie PDF (Barrierefreie Gestaltung von Internetangeboten)
- Weitergabekontrolle durch Einrichtungen der Datenübertragung
- Verschlüsselung von Datenbanken
- Dokumentenmanagement mit Versionierungssystem
- E-Mail-Gateway mit Filterfunktionen
- Eingabekontrolle bei Datenverarbeitungssystemen
- Übergabepunkte und Ladezonen sind von den Räumen, in denen die Datenverarbeitungsanlagen untergebracht sind, separiert.
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von Virenschutzlösung/ Regelmäßige Aktualisierung des Virenschutzprogramms
- Externe Dateien und Ordner auf Viren untersuchen (Online-Virenscanner / Antivirenprogram)

Verfügbarkeit

- Regelungen für die Durchführung der Datensicherungen (Backups)
- Instandhaltung Technischer Anlagen und Komponenten (Ausfallsicherheit)
- Sicherstellung der Langzeitarchivierung und Verfügbarkeit durch Umspeicherung verschlüsselter Daten auf andere Datenträger zur Gewährleistung der Prüf- und Lesbarkeit
- Vertretungsregelung Administrator
- Versorgungsleitungen (Strom, Breitband, Gas, Wasser, sonst. Meldeleitungen)
- Verringerung der Brandlasten im Raum der Datenverarbeitung
- Verantwortliche (z. B. Admins) werden durch automatisierte Alarmsysteme über einen System-Ausfall informiert
- Weitestgehender Verzicht auf Makros in Office-Dokumenten
- Zugriffsrechte orientieren sich an Zuständigkeiten
- Wartung der IT-Infrastruktur (Ausfallsicherheit)
- Sicherheits-Stromversorgung/Notstromanlagen (Notstrom-Systeme)
- Verfügbarkeitskontrolle bei der Verarbeitung personenbezogener Daten
- Stromkreise
- Unterbrechungsfreie Stromversorgung (USV)
- Das Klima der Räume in denen Datenverarbeitungsanlagen (z. B . Serverraum) stehen werden klimatisch überwacht und das Klima wird (automatisiert) geregelt.
- Auto-Start von externen Medien ist deaktiviert, die Verwendung externer Medien erheblich eingeschränkt.
- Die IT-Systemlandschaft ist umfangreich dokumentiert
- Dokumentation des Datenschutz-Management-Systems (DSMS) in der Robin Data Software
- Einsatz von Content Management Systemen (CMS)
- Festgelegte Zuständigkeiten im Rahmen der Datensicherung
- Feuerlöscher sind für die Räume der Datenverarbeitungsanlage vorhanden
- Gefährdungsschutz (Naturkatastrophen) für Rechenzentrum (RZ) sowie Serverraum
- Festplattenvollverschlüsselung bei PCs und Notebooks (Hardwaregestütze Verschlüsselung)
- Dokumentation des Datenschutz-Management-Systems (DSMS) in der Robin Data Software
- Rauchmeldeanlagen im Raum der Datenverarbeitungsanlagen
- Raum der Datenverarbeitungsanlagen ist klimatisiert
- Penetration Tests (Schwachstellenanalyse - Penetration IT-System, Webseite, Cloudlösungen)
- Personalrisiken erkennen und begegnen (Personalrisikomanagement)

Belastbarkeit

- One-Premise-Lastenausgleich der Server
- Lastenausgleich der Netzwerkkomponenten
- Lastenausgleich für SaaS-Lösungen
- Bei hochverfügbaren Lösungen erfolgt ein Cloud-basierter Lastenausgleich per virtualisierten Server, die in einem sicheren Land gehostet werden.
- Installation verfügbarer Sicherheitsupdates
- Überspannungsschutz
- Die Räume mit den Datenverarbeitungsanlagen sind baulich geeignet (z. B. Lambertz-Zelle, nicht im feuchten Keller, vor unbefugtem Zutritt geschützt).

Rechenschaftspflichten

- Bei Anbietern von Videokonferenzsystemen in unsicheren Drittstaaten sind geeignete Garantien vorhanden.

- Zugriff und Auswertung der Aufzeichnungen der Videoüberwachung
- Vertretungsregelung Datenschutzbeauftragter
- Administration der Videoüberwachung - Privacy by default (Datenschutzfreundliche Voreinstellungen)
- Bei Videokonferenzen kann der Hintergrund eines Nutzers softwareseitig unscharf gestellt werden (Blurring)
- Auftragskontrolle bei der Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung / AV-Vertrag)
- Dienstlich zur Verfügung gestellte Geräte werden nicht für private Zwecke genutzt.
- Die Tätigkeiten der Datenschutzzuständigen werden dokumentiert
- Zugriff und Auswertung der Aufzeichnungen der Videoüberwachung
- Administration der Videoüberwachung - Privacy by default (Datenschutzfreundliche Voreinstellungen)
- Ein Datenschutzbeauftragter (extern) ist bestellt und kann weisungsfrei agieren.
- Dokumentation Erste-Hilfe-Maßnahmen (Organisation des Arbeitsschutzes)
- Prozess der Meldung einer Datenschutzverletzung (Datenpanne)
- Regelmäßige Audits zur Überprüfung der Wirksamkeit der Datenschutzmaßnahmen
- Regelmäßige Auswertung und Prüfung der Serverprotokolle
- Netztrennung zwischen den WLAN-Netzen – Maßnahmen für einen sicheren WLAN-Betrieb
- Täglich Updates der Virensignaturen auf den Clients sind gewährleistet.
- Festlegung und Kommunikation der Zuständigkeiten im Update- und Patchmanagement
- Home-Office / Telearbeit: Einsatzplanung im Home Office (Mitarbeiterübersicht)
- Kontinuierliche Aktualisierung des Datenschutz-Management-Systems (DMS)
- Führen des Verzeichnisses der Verarbeitungstätigkeiten (Verfahrensverzeichnis)
- Entfernung von Eigentum des Unternehmens
- Regelmäßig dokumentierte Schulungen der Mitarbeiter auf den Datenschutz.
- Digitales Equipment wird vom Arbeitgeber gestellt
- Dokumentation getroffener Sicherheitsmaßnahmen (VV, TOMs)
- Eine Datenschutzorganisation ist in der Organisation etabliert (mit oder ohne DSB)
- Dokumentation der vorhandenen IT-Infrastruktur und der Schutzbedarfe
- Die automatische Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten wird durch die Konfiguration unterbunden.

Nicht-Verkettung

- Logische Mandantentrennung
- Trennungsgebot bei der Verarbeitung personenbezogener Daten

Dokumentenhistorie

Version	Datum	Autoren	Änderung
1.0	07.04.2018	H. Fierdag	INIT
1.1	12.06.2021	H. Fierdag	Aufnahme & Erweiterung TOM‘s
1.2	03.11.2023	Y. Hoffmann	Aktualisierung TOM’s & Dienstleister
1.3	29.12.2024	Y. Hoffmann	Aktualisierung TOM’s & Dienstleister
2.0	07.05.2025	K. Steger	Überarbeitung der gesamten AVV
2.1	18.16.2025	T.Polster	Aktualisierung der Schlussbestimmungen
2.2	18.11.2025	K.Steger	Anpassung der AVV Strutur
2.3	19.03.2026	K.Steger	Ergänzung Dienstleister für SaaS Anwendung und Klausel zur Nutzung von Auftraggeber Daten für statstische Zwecke sowie Anpassung des Formats des AVVs, damit dieser automatisch im Hauptvertrag miteinbezogen wird.