Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

Kunde

- Auftraggeber -

und

Offpaper GmbH
Elmer-Fryar-Ring 26
86391 Stadtbergen

- Auftragnehmer –

1. Allgemeines

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

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

2. Gegenstand des Auftrags

Der Gegenstand 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. 10 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 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.

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.

(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 2 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei 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.

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

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

17. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

(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.

Stand: 08.01.2025

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber eine SaaS (Software as a Service)-Software zur digitalen Erstellung von Formularen zur Datenerfassung, PDF-Berichten zur Darstellung der erfassten Daten und Automationen zur Weiterverarbeitung der erfassten Daten zur Verfügung. Die Nutzung der Software erfolgt browserbasiert über das Internet. Die Formulare zur Datenerfassung können sowohl browserbasiert als auch mit der zusätzlich zur Verfügung gestellten mobilen App für IOS und Android befüllt und abgesendet werden. Die erfassten Daten werden in der Cloud des Auftragnehmers gespeichert. Welche Daten erfasst werden, wird durch den Auftraggeber festgelegt, ebenso der Inhalt des daraus generierten Berichts sowie die Art und Weise der Weiterverarbeitung. Der Auftraggeber hat die Möglichkeit, die erfassten Daten und daraus generierte Berichte über vorhandene Schnittstellen an Dritte zur Verarbeitung weiterzugeben. Der Auftragnehmer hat darauf keinen Einfluss.

Weitergehende Informationen zum Gegenstand ergeben sich aus dem Hauptvertrag.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind Gegenstand dieses Auftrags:

- Personenstammdaten (Vorname, Nachname, Anwenderrolle bzw. Berechtigungen der Nutzer / zusätzlich Kontaktdaten inkl. Telefonnummer des Ansprechpartners)
- Kommunikationsdaten (E-Mail-Adresse, IP-Adresse)
- Nutzungsdaten (Logins, Browser-Typ, Zeitpunkt, an dem ein Formular von einem Nutzer als Entwurf in der Cloud gespeichert oder abgesendet wird)
- Technische Daten (Betriebssystem, Typ und Modell des genutzten Geräts, auf Anforderung auf dem Gerät gespeicherte Fehlerprotokolle, API-Aufrufe, Server-Logs)
- Support- und Servicedaten (Support-Tickets, Anfragen über E-Mail oder Chat-Bot, Angaben zur Problemlösung)

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, insofern sie vom Auftraggeber als Nutzer der Software des Auftragnehmers angelegt wurden
- Ggf. Dienstleister, Subunternehmer, Lieferanten oder weitere Dritte, insofern sie vom Auftraggeber als Nutzer der Software des Auftragnehmers angelegt wurden

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**	**Server-Standort**	**Datenübermittlung in Drittstaaten (Rechtsgrundlage)**
Microsoft Ireland Operations Ltd.	One Microsoft Place, Leopardstown, Dublin 18, Ireland	Cloud Serverhosting über die Microsoft Azure Cloud	Frankfurt, Deutschland	Angemessenheitsbeschluss / EU Standardvertragsklauseln
MongoDB Limited	Building 2, Number One Ballsbridge, Shelbourne Rd, Ballsbridge, Dublin 4, D04 Y3X9, Irland	Cloud Datenspeicherung	Frankfurt, Deutschland	-
Supabase Inc.	970 Toa Payoh North #07-04, Singapore 318992	Authentifizierung, Login-Prozess	Frankfurt, Deutschland	EU Standardvertragsklauseln
Gleap GmbH	Dr. Walter-Zumtobel-Straße 2, 6850-Dornbirn, Österreich	Chat-Support, Hilfe- und Support-Center	Frankfurt, Deutschland	-
ConvertAPI, UAB	Lauksargio 111, Vilnius, LT-10105, Lithuania	Dokument-Konverter	Frankfurt, Deutschland	-

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Die Datenverarbeitung des Auftragnehmers geschieht in Übereinstimmung mit den gesetzlichen Vorgaben zur Auftragsverarbeitung im Sinne von Art. 28 DSGVO. Die folgenden Ausführungen stellen die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO dar.

1. Vertraulichkeit

(1) Zutrittskontrolle

Die Büroräume der Firma Offpaper GmbH sind durch ein elektronisches Schließsystem gegen unbefugten Zutritt geschützt. Der Zutritt ist nur mit einem kryptografischen Schlüssel möglich, der mittels Chip oder App an berechtigte Mitarbeiter ausgehändigt wird. Darüber hinaus ist es den Mitarbeitern gestattet, von zuhause aus bzw. Remote zu arbeiten. Sie wurden über die damit verbundenen datenschutzrechtlichen Verpflichtungen belehrt und sind verpflichtet, den in der „Sicherheitsrichtlinie Telearbeit“ auf Basis der ‚BSI-Empfehlung zur Cyber-Sicherheit‘ (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf) festgehaltenen betrieblichen Regelungen Folge zu leisten.

(2) Zugangs- und Zugriffskontrolle

Die Datenverarbeitung der Offpaper GmbH findet auf Servern der Microsoft Corporation (Azure Cloud) in Frankfurt/Deutschland statt. Die Microsoft Azure Cloud ist nach dem internationalen Standard für den Datenschutz in der Cloud (ISO/IEC 27018) sowie nach Information Security Management Standards (ISO/IEC 27001) zertifiziert und wird regelmäßig rezertifiziert. Dementsprechend gelten die dort implementierten technischen und organisatorischen Maßnahmen ebenso für die Systeme der Offpaper GmbH.

Gleiches gilt für die Datenspeicherung der Offpaper GmbH auf den Servern der MongoDB Atlas Cloud in Frankfurt/Deutschland. Diese ist ebenfalls nach dem internationalen Standard für den Datenschutz in der Cloud (ISO/IEC 27018) sowie nach Information Security Management Standards (ISO/IEC 27001) zertifiziert.

Der Zugang zu DV-Anlagen, auf denen Daten verarbeitet werden, ist erst nach Identifikation und erfolgreicher Authentisierung der befugten Personen möglich. Passworte entsprechen angemessenen Mindestregeln hinsichtlich der minimalen Passwortlänge und Komplexität. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden. Die Umsetzung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit wird durch technische Einstellungen sichergestellt. Alle erfolgreichen und abgewiesenen Zugangsversuche werden protokolliert. Nach wiederholter fehlerhafter Authentisierung wird der Zugang gesperrt.

Die Vergabe von Zugangsberechtigungen erfolgt immer nur für diejenigen DV-Anlagen, zu welchen der Zugang im Rahmen der Aufgabenwahrnehmung notwendig ist ("Prinzip der minimalen Berechtigung"). Authentifizierungsmedien und/oder Benutzerkennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür sensibilisiert.

Der Kreis der Personen, die befugt Zugriff auf DV-Anlagen erhalten, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum beschränkt. Zugänge für temporär beschäftigte Personen werden individuell vergeben. Wieder verwendbare Kennungen werden nicht vergeben.

Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. Der Zugriff auf Kundendaten ist darüber hinaus nur Personen erlaubt, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.

(3) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt verarbeitet. Der Zweck der Datenerhebung wird durch den Kunden durch die individuelle Nutzung seines Offpaper-Kontos festgelegt. Offpaper gewährleistet die logisch getrennte Speicherung von und den getrennten Zugriff auf Kundendaten für jedes Offpaper-Konto.

(4) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Der Auftragnehmer verarbeitet zum Zweck der Berechtigungs- und Zugangssteuerung des Kundenkontos nur ein Minimum an personenbezogenen Daten des Auftraggebers. Diese können daher nicht pseudonymisiert werden. Eine darüber hinaus gehende Pseudonymisierung von durch den Auftraggeber im Rahmen der Nutzung erhobenen bzw. gespeicherten personenbezogenen Daten ist von diesem selbst vorzunehmen, soweit dies möglich und datenschutzrechtlich erforderlich ist.

(5) Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Der Zugriff auf die Daten der eingesetzten Software ist nur über verschlüsselte Zugangsverfahren möglich. Die Datenübertragung von und zu der Offpaper Cloud Plattform erfolgt grundsätzlich SSL-verschlüsselt. Die Speicherung der Daten erfolgt ebenfalls ausschließlich verschlüsselt.

2. Integrität

(1) Weitergabekontrolle

Die Datenübertragung von mobilen Endgeräten der Nutzer des Auftraggebers in die Systeme zur Datenverarbeitung des Auftragnehmers (Microsoft Azure Cloud) erfolgt ausschließlich über SSL-verschlüsselte Verfahren (https-Protokoll).

Die IT-Systeme, auf denen personenbezogene Daten verarbeitet werden, werden durch geeignete Maßnahmen (u.a. Firewalls) vor unbefugtem Zugriff und Datenentwendung geschützt. Die Backendsysteme werden regelmäßig gewartet und mit Updates und Security-Fixes versehen, um unbefugten Zugriff durch das Ausnützen von Sicherheitslücken zu verhindern.

Eine Speicherung personenbezogener Daten auf mobilen Datenträgern durch den Auftragnehmer findet nicht statt.

Der Export von Daten über von der Software des Auftragnehmers angebotene Exportmöglichkeiten (Webhook, Excel-Export) durch den Auftraggeber und deren Weiterverarbeitung in Systemen des Auftraggebers unterliegt der alleinigen Verantwortung des Auftraggebers.

Jegliche Art der Vervielfältigung von Daten, Datenträgern oder Unterlagen des Auftraggebers ist unzulässig, sofern dies nicht explizit Bestandteil der Auftragsausführung ist. In diesem Fall werden Kopien ausschließlich für die vom Auftraggeber festgelegten Zwecke sowie in dem hierfür erforderlichen Umfang angefertigt werden.

Die Weitergabe von Kundendaten an Subunternehmer ist nur mit Genehmigung des Auftraggebers möglich. Hierfür werden ausschließlich Subunternehmer herangezogen, die hinreichende Garantien dafür bieten, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt.

(2) Eingabekontrolle

Zur Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege werden sämtliche Zugriffe auf die Daten protokolliert. Ein Protokollauswertungssystem steht zur Verfügung.

3. Verfügbarkeit und Belastbarkeit

(1) Verfügbarkeitskontrolle

Offpaper sichert alle Kundendaten regelmäßig auf Basis eines Backup-Konzepts. Auf Basis einer Sicherung können die Kundendaten im Notfall in angemessener Zeit wiederhergestellt werden. Backups werden bis zu einer Dauer von 35 Tagen vorgehalten.

Die Häufigkeit der Sicherung wird im Hauptvertrag geregelt. Die Ablage erfolgt verschlüsselt und physisch an einem anderen Ort als an dem Ort, an dem sich die Daten primär befinden.

Der Auftraggeber wird über jede mehr als unerhebliche Störung (z. B. vorsätzlicher Angriff intern/extern) und Außerbetriebnahme der Datenverarbeitung schnellstmöglich informiert.

(2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

Die Datenwiederherstellungsverfahren werden regelmäßig geprüft. Alle Datenwiederherstellungsmaßnahmen werden protokolliert. MongoDB Atlas als für die Datenspeicherung verantwortlicher Subunternehmer definiert hierfür Verfahren, die sicherstellen, dass Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung wiederhergestellt werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(1) Datenschutz-Management

Offpaper verfügt über ein Datenschutz-Management, um die datenschutzrechtlichen Vorgaben nach §§ 5, 30, 32 und 35 DSGVO zu erfüllen. So wurden geeignete technische und organisatorische Maßnahmen umgesetzt, um sicherzustellen, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt. Ein Datenschutzbeauftragter wurde bestellt. Alle Mitarbeiter werden arbeitsvertraglich auf das Datengeheimnis verpflichtet und regelmäßig im Datenschutz geschult.

Die für die Auftragsverarbeitung genutzten bzw. währenddessen erhobenen und verarbeiteten Daten werden, soweit dies möglich ist, unwiderruflich gelöscht oder gegen weitere Zugriffe gesperrt, wenn die Beauftragung zur Verarbeitung endet. Die Fristen ergeben sich aus den vertraglichen Vereinbarungen mit den Auftraggebern und Lieferanten, soweit nicht gesetzliche Vorgaben die Grundlage für Löschfristen bilden.

(2) Incident-Response-Management

Im Falle eines datenschutzrelevanten Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten, der die Einleitung angemessener Maßnahmen vorschlägt.

(3) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die für die Auftragsverarbeitung genutzten bzw. währenddessen erhobenen und verarbeiteten Daten werden nur im für den jeweiligen bestimmten Verarbeitungszweck erforderlichen Umfang erhoben und gespeichert und nur den Personen zugänglich gemacht, die diese Informationen für den jeweiligen Verarbeitungszweck benötigen. Soweit dies möglich ist, werden die verarbeiteten Daten unwiderruflich gelöscht oder gegen weitere Zugriffe gesperrt, wenn die Beauftragung zur Verarbeitung endet. Die Fristen ergeben sich aus den vertraglichen Vereinbarungen mit den Kunden und Lieferanten, soweit nicht vorrangige gesetzliche Vorgaben die Grundlage für Löschfristen bilden.

(4) Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO geschieht ohne entsprechende Weisung des Auftraggebers. Die weisungsgemäße Auftragsverarbeitung wird durch die Vertragsgestaltung gesichert. Zudem müssen mündlich erteilte Weisungen unmittelbar im Nachgang per E-Mail oder brieflich bestätigt werden. Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.