Vereinbarung zur Verarbeitung von personenbezogenen Daten im Auftrag (AV) nach Art 28 DSGVO

zwischen

<FIRMA_AUFTRAGGEBER>
vertreten durch: <NAMEN>
<ADRESSE_AUFTRAGGEBER>
- nachstehend Auftraggeber genannt -

und der

Papershift GmbH, Registergericht Mannheim, HRB 722151
Lange Straße 2, 76199 Karlsruhe
vertreten durch die Geschäftsführung: Michael Emaschow, Florian Suchan
- nachstehend Auftragnehmerin genannt -

1. Gegenstand und Dauer der Vereinbarung

1.1. Gegenstand der Vereinbarung

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem, zwischen den Parteien über die Webseite app.papershift.com geschlossenen, Vertrag (im Folgenden: Nutzungsvertrag) in ihren Einzelheiten ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Dienstleistungsvertrag in Zusammenhang stehen und bei denen Beschäftigte der Auftragnehmerin oder durch die Auftragnehmerin Beauftragte mit personenbezogenen Daten, für die der Auftraggeber verantwortliche Stelle oder selbst Auftragnehmerin ist (im Folgenden: personenbezogene Daten des Auftraggebers), in Berührung kommen können. Soweit Regelungen der hier vorliegenden Vereinbarung den Regelungen des Nutzungsvertrags widersprechen, gehen die Regelungen der hier vorliegenden Vereinbarung vor.

Die Auftragnehmerin erbringt die folgende Dienstleistung: Die entgeltliche Bereitstellung von Leistungen durch die Auftragnehmerin im Rahmen des Nutzungsvertrags, insbesondere die Zurverfügungstellung einer Dienstplanungs- und Personalplaner-Software als Software as a Service (SaaS).

Gegenstand des Auftrags ist jedoch nicht die originäre Verarbeitung von personenbezogenen Daten durch die Auftragnehmerin. Im Zuge der Leistungserbringung durch die Auftragnehmerin als Dienstleisterin wird jedoch auf personenbezogene Daten des Auftraggebers Zugriff genommen.
Somit verarbeitet die Auftragnehmerin personenbezogene Daten im Auftrag des Auftraggebers (Auftragsverarbeitung im Sinne von Artikel 28 DSGVO[1]).

1.2. Dauer der Vereinbarung

Die Dauer dieser Vereinbarung richtet sich nach der Laufzeit des Nutzungsvertrags.

2. Zweck und Daten

2.1. Art und Zweck der Verarbeitung

Der Auftraggeber verarbeitet personenbezogene Daten im Rahmen seiner im Nutzungsvertrag beschriebenen Tätigkeit. Von der Auftragstätigkeit sind die im Folgenden beschriebenen Datenkategorien in dem sich aus dem Nutzungsvertrag ergebenen Umfang und Zweck betroffen: Das System erlaubt die Erfassung von personenbezogenen Daten, insbesondere abrechnungsrelevante Daten, wie z.B. Arbeitszeiten, Zeiterfassungen, Urlaubstage, Kranktage, sonstige Fehlzeiten, Vertragskonditionen, Stundenlohn. Der Auftraggeber kann darüber hinaus im System selbstständig eigene Datenfelder konfigurieren. Der Auftraggeber möchte davon folgende Personenbezogene Daten von Mitarbeitern erheben:

- Nutzungsdaten, die bei der Nutzung des Services durch die Nutzer anfallen.
- Sensitive Daten, soweit dies im Rahmen der von der Auftragnehmerin übernommenen Tätigkeit erforderlich ist.

2.2. Kategorien betroffener Personen
Personal, wie z.B. Bewerber, Beschäftigte.

3. Pflichten und Rechte des Auftraggebers

3.1. Die Beurteilung der Zulässigkeit der Datenverarbeitung und die Wahrung der Rechte der Betroffenen ist die Pflicht des Auftraggebers.

3.2. Jeder Weisung bedarf der Schriftform.

3.3. Der Auftraggeber hat das Recht, Weisungen zu erteilen, die die Datenverarbeitung betreffen, insbesondere die unter 7 genannten sowie die Rückgabe von Daten. Die

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); gültig ab 25.05.2018

Weisung, Daten endgültig zu löschen bleibt bis zum Vertragsende dem Auftraggeber vorbehalten.

3.4. Falls Weisungen die getroffenen Festlegungen dieses Vertrages ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

4. Pflichten der Auftragnehmerin

4.1. Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers. Die Auftragnehmerin darf die zur Verarbeitung überlassen Daten nicht für andere Zwecke verarbeiten oder nutzen. Die Auftragnehmerin ist nicht befugt, eigenmächtig Veränderungen an den Daten vorzunehmen.

4.2. Mündliche Weisungen sind zu ignorieren, jede Weisung bedarf der Schriftform (E-Mail genügt).

4.3. Die Verarbeitung und Nutzung der Daten findet möglichst im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Soweit Cloud-Dienste (z.B. Amazon Cloud) eingesetzt werden, stellt die Auftragnehmerin sicher, dass die Daten innerhalb des EWR verbleiben oder entsprechende Garantien entsprechend dem Kapitel V der DSGVO gegeben sind. Jede Verlagerung in ein Drittland, die über das bisher genehmigte Maß hinausgeht, ist dem Auftraggeber mit einer Frist von sechs Wochen anzuzeigen.

4.4. Die Auftragnehmerin verpflichtet sich, bei der Verarbeitung der Daten des Auftraggebers die Vertraulichkeit zu wahren. Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter auf die Vertraulichkeit gemäß Art. 29 DSGVO verpflichtet (ehemals Datengeheimnis gemäß § 5 BDSG). Die Auftragnehmerin bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und überwacht deren Einhaltung. Hierzu verwendet er das Formular aus dem Anhang „Verpflichtung auf das Datengeheimnis“ und macht sie mit den maßgebenden Bestimmungen des Datenschutzes vertraut.

4.5. Die Auftragnehmerin kontrolliert regelmäßig die Verpflichtung auf das Datengeheimnis und die Einhaltung der technischen und organisatorischen Maßnahmen.

4.6. Ist die Auftragnehmerin der Ansicht, dass eine Weisung des Auftraggebers gegen eine Vorschrift verstößt, hat er den Auftraggeber unverzüglich darauf

hinzuweisen. Er ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4.7. Die Auftragnehmerin darf die Daten nicht länger speichern, als der Auftraggeber schriftlich bestimmt hat (Ausschluss von Aufbewahrungspflichten z.B. nach HGB).

4.8. Die Auftragnehmerin hat einen Datenschutzbeauftragten zu benennen. Seine Kontaktdaten, sowie ein Wechsel ist dem Auftraggeber anzuzeigen. Siehe Anhang „Zu benennende Personen (Weisungsbefugte, DSB)".

5. Technische und organisatorische Maßnahmen

5.1. Die Auftragnehmerin beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

5.2. Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen (entsprechend Art 32 DSGVO) werden als verbindlich festgelegt.

5.3. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Sofern bei dieser Anpassung das Schutzniveau erhalten bleibt oder verbessert wird, ist der Auftraggeber nicht gesondert zu informieren, wesentliche Änderungen sind dem Auftraggeber schriftlich anzuzeigen. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

5.4. Der Auftraggeber kann durch Weisung eine Ergänzung der technischen und organisatorischen Maßnahmen verlangen. Entstehen Kosten hat der Auftraggeber zu tragen.

6. Unterauftragnehmer

Die Beauftragung von Subunternehmern ist ausschließlich unter folgenden Bedingungen erlaubt:

6.1. Die Auftragnehmerin teilt Namen, Anschrift und Art der Dienstleistung des Subunternehmers dem Auftraggeber mit. Die im Anhang „Unterauftragnehmer" aufgeführten Subunternehmer gelten als genehmigt.

6.2. Außerdem muss die Auftragnehmerin versichern, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung und der von ihm getroffenen organisatorisch-technischen Maßnahmen ausgewählt hat. Die Auftragnehmerin hat die Einhaltung derselben beim Subunternehmer regelmäßig zu überprüfen: Das Ergebnis der Überprüfungen ist zu dokumentieren und auf Anfrage an den Auftraggeber weiterzuleiten.

6.3. Die Auftragnehmerin hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmerin auch gegenüber Subunternehmern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen, wenn das beauftragte Subunternehmen nicht über Zertifikate im Sinne von § 10.2 dieser Vereinbarung verfügt.

6.4. In dem Vertrag mit dem Subunternehmer sind die Verantwortlichkeiten der Auftragnehmerin und des Subunternehmers deutlich voneinander abzugrenzen. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

6.5. Die Auftragnehmerin informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen schriftlich (E-Mail genügt) Einspruch zu erheben. Ein wichtiger Grund liegt insbesondere dann vor, wenn ernsthafte und seitens der Auftraggeberin zu begründende Zweifel daran bestehen, dass der betreffende Subunternehmer einen nach Maßgabe der einschlägigen gesetzlichen Regelungen ausreichenden Schutz der zu verarbeitenden Daten gewährleisten kann. Im Falle eines solchen Einspruchs werden die Vertragsparteien auf eine gütliche Einigung hinwirken. Sollte binnen 4 Wochen keine für die Auftraggeberin akzeptable Lösung gefunden werden, so kann Auftraggeberin entweder die Abschaltung der nicht betriebsnotwendigen Subunternehmer Tools veranlassen oder ihr steht alternativ ein Sonderkündigungsrecht zu.

6.6. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach Art 28 DSGVO erfüllt hat. Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet die Auftragnehmerin gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

6.7. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen und Reinigungskräfte.

7. Betroffenenrechte

7.1. Die Auftragnehmerin hat personenbezogene Daten zu berichtigen, zu löschen oder zu sperren, sowie den Auftraggeber bei seinen Pflichten zur Information, Auskunft, Datenübertragbarkeit und Widerspruch zu unterstützen, wenn der Auftraggeber dies in einer Weisung verlangt. Entsprechende Anfragen von Betroffenen oder Dritten sind an den Auftraggeber weiterzuleiten.

7.2. Sofern nicht anders vereinbart, trägt der Auftraggeber entstehende Kosten. Diese sind dem Auftraggeber vorher mitzuteilen.

8. Unterstützung bei Pflichten des Auftraggebers

8.1. Die Auftragnehmerin unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Diese sind:

- Sicherheit der Verarbeitung
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
- Datenschutz-Folgenabschätzung
- Vorherige Konsultation

8.2. Sofern die Auftragnehmerin den Umstand nicht zu verantworten hat, trägt der Auftraggeber entstehende Kosten. Diese sind dem Auftraggeber vorher mitzuteilen. Bei Art. 32 DSGVO ist davon auszugehen, dass die Auftragnehmerin dies zu verantworten hat, bei einer Datenschutzverletzung dann, wenn sich die Verletzung bei der Auftragnehmerin ereignete.

9. Löschung bei Vertragsende

9.1. Nach Abschluss der vertraglichen Arbeiten hat die Auftragnehmerin sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse (Daten und Datenträger), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder bzw. und zu löschen/vernichten.

9.2. Alle Daten und ergänzend hinzugewonnenen personenbezogenen Daten/Unterlagen des Auftraggebers in Systemen der Auftragnehmerin, die nicht mehr benötigt werden, sind unwiderruflich zu löschen bzw. zu vernichten. Die Löschung betrifft nicht nur die Nutzsysteme, sondern auch alle damit verbundenen Dateien und Daten in allen Systemen und auf allen Speichermedien, insbesondere Backups, der Auftragnehmerin. Datenträger (Papier, Festplatten, CD's, USB-Sticks usw. einschließlich sämtlicher Fehldrucke bzw. Fehlspeicherungen), die Daten des Auftraggebers enthalten, sind nach DIN-Norm 66399 zu vernichten.

9.3. Die Auftragnehmerin ist verpflichtet, organisatorisch sicherzustellen, dass die Daten des Auftraggebers auch tatsächlich gelöscht bzw. vernichtet werden können. Die Auftragnehmerin hat sämtliche Beschäftigten über diese Löschpflichten zu informieren.

10. Kontrollrecht

10.1. Der Auftraggeber ist berechtigt und verpflichtet, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der bei der Auftragnehmerin getroffenen technisch-organisatorischen Maßnahmen (siehe Anhang) zu überzeugen.

10.2. Dies erfolgt durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen, einer Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits oder durch Inspektion bei der Auftragnehmerin.

10.3. Die Auftragnehmerin erteilt entsprechende Auskünfte.

10.4. Der Auftraggeber kann nach Ankündigung während der üblichen Geschäftszeiten Besichtigungen und Prüfungen vornehmen. Er kann diese Kontrolle auch durch einen Dritten durchführen lassen. Die Auftragnehmerin sichert zu, dass er an diesen Kontrollen mitwirkt. Sofern nicht anders vereinbart, trägt der Auftraggeber entstehende Kosten. Diese sind dem Auftraggeber vorher mitzuteilen.

10.5. Im Rahmen dieser Prüfung darf der Auftraggeber prozessbezogene Unterlagen sowie seine gespeicherten Daten und die Datenverarbeitungsprogramme einsehen.

11. Meldung einer Verletzung des Schutzes personenbezogener Daten an den Auftraggeber

11.1. Die Auftragnehmerin teilt dem Auftraggeber unverzüglich, jedoch spätestens innerhalb von 24 Stunden, nachdem ihm die Verletzung bekannt wurde, mit:

- Den Verdacht auf Verletzungen der Vertraulichkeit der Daten,
- Verstöße der Auftragnehmerin oder der bei ihm beschäftigten Personen gegen
- datenschutzrechtliche Bestimmungen,
- die im Auftrag getroffenen Festlegungen oder
- den nicht wiederherstellbaren Verlust oder Fehlerhaftigkeit von Daten.

Hierzu sind die Angaben nach dem Anhang „Meldung von Datenschutz verletzungen“ zu machen.

11.2. Die Auftragnehmerin trifft erforderliche Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen. Sie unterstützt den Auftraggeber bei der Erfüllung von Informationspflichten nach Art. 33 und 34 DSGVO.

12. Verschwiegenheitspflicht

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln.

13. Verhältnis zum Hauptvertrag / Kündigung

13.1. Eine gesonderte Kündigung dieser Vereinbarung ohne gleichzeitige Beendigung des Hauptvertrages ist ausgeschlossen.

13.2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen die Bestimmungen dieses Vertrages vorliegt, die Auftragnehmerin eine gesetzeskonforme Weisung des Auftraggebers nicht ausführen kann oder will oder die Auftragnehmerin den Zutritt des Auftraggebers vertragswidrig verweigert.

14. Pfändung, Beschlagnahme bei der Auftragnehmerin

Sollte das Eigentum des Auftraggebers bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin den Auftraggeber unverzüglich zu verständigen.

15. Zurückbehaltungsrecht an personenbezogenen Daten

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen.

16. Ort der Verarbeitung, Sicherung

16.1. Die Verarbeitung von Daten findet möglichst nur innerhalb der EU bzw. des EWR statt (vgl. 4.3).

16.2. Die Verarbeitung von Daten in Privatwohnungen ist gestattet, wenn ein Kontrollrecht gewährleistet wird.

16.3. Die Übertragungswege sind zu sichern (verschlüsseln). Die Art und Weise ist im Anhang „Zu benennende Personen “ festgelegt.

17. Haftung, Schadensersatz und Vertragsstrafe

17.1. Haftung und Schadensersatz richten sich nach den gesetzlichen Regelungen (Art. 82 DSGVO).

17.2. Die Auftragnehmerin haftet dem Auftraggeber für Schäden, die die Auftragnehmerin, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

17.3. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG bzw. DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich, dem Auftraggeber bleibt der Rückgriff zur Auftragnehmerin vorbehalten.

18. Verzeichnis von Verarbeitungstätigkeiten bei der Auftragnehmerin

Diese Vereinbarung enthält für diese Auftragsverarbeitung alle Angaben nach Art. 30 Abs. 2 DSGVO:

- Auftragsverarbeiter: Siehe Angaben zur Auftragnehmerin (am Beginn dieser Vereinbarung)
- Verantwortlicher: Siehe Angaben zum Auftraggeber (am Beginn dieser Vereinbarung)
- Kategorien von Verarbeitung: Siehe Kapitel 2 „Zweck und Daten“
- Übermittlungen an ein Drittland: Siehe Kapitel 4.3 und Kapitel 16 „Ort der Verarbeitung, Sicherung“
- Technische und organisatorische Maßnahmen: Siehe Anhang „Technische und organisatorische Maßnahmen bei der Auftragnehmerin“

19. Salvatorische Klausel

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich stattdessen zur Vereinbarung einer Ersatzregelung, welche der ungültigen oder undurchführbaren in gesetzlich zulässiger und wirtschaftlicher Weise in deren Wirkungen am nächsten kommt. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Zusatzvereinbarung als lückenhaft erweist.

20. Weisungsbefugte

Weisungsempfänger bei der Auftragnehmerin sind Herr Florian Suchan und Herr Michael Emaschow. Die weisungsbefugten Personen des Auftraggebers sind die im Rubrum dieser Vereinbarung genannten Vertretungsberechtigten sowie die von Ihnen schriftlich benannten Personen.

21. Nebenabreden

Zum Zeitpunkt des Vertragsabschlusses bestehen keine Nebenabreden. Für Nebenabreden zu diesem Vertrag ist die Schriftform erforderlich. Dazu gehört auch die Aufhebung dieser Schriftformklausel.

Folgende Anhänge gehören zur Vereinbarung:

- Anhang Technische und organisatorische Maßnahmen bei der Auftragnehmerin
- Anhang Unterauftragnehmer
- Anhang Zu benennende Personen
- Anhang Meldung von Datenschutzverletzungen
- Anhang Verpflichtung auf das Datengeheimnis