Vertrag zur Auftragsverarbeitung

Zwischen

Name of Company
Address line 1
Address line 2

im Folgenden **Auftraggeber/AG** genannt

und

Layer Software GmbH
Manteuffelstr 77
10999 Berlin

im Folgenden **Auftragnehmer/AN** genannt

§ 1 Vertragsgegenstand

Dieser Vertrag regelt die Verarbeitung der personenbezogenen Daten der Kunden des Auftraggebers, die der AN im Rahmen der Erbringung der Leistungen für den AG verarbeitet ("Daten").
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der AG verantwortlich.

§ 2 Art und Zweck der Datenverarbeitung des Auftraggebers

(1) Art und Zweck der Verarbeitung
Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

Die Verarbeitung dient folgendem Zweck: Der AN ermöglicht eine erleichterte Zusammenarbeit innerhalb des Unternehmens mit Excel und Google Sheet Dateien. Dies beinhaltet das interne Teilen von Excel Dateien, sowie die vereinfachte Bearbeitung. Dies wird durch das eigens entwickelte Tool ermöglicht.

(2) Art der Daten
Es werden folgende Daten verarbeitet:
- Personenstammdaten (Anrede, Name, Adresse, Lieferadresse, Telefon, E-Mail)

(3) Kategorien der betroffenen Personen
Von der Verarbeitung betroffen sind:
- Mitarbeiter

§ 3 Pflichten des Auftragnehmers

(1) Der AN verpflichtet sich die Vorschriften der einschlägigen Datenschutzgesetze zu befolgen und die Grundsätze ordnungsmäßiger Datenverarbeitung zu beachten

(2) Der AN verarbeitet die Daten ausschließlich im Rahmen und zum Zwecke der Erbringung der Leistungen für den AG und nach dessen dokumentierten Weisungen. Kopien oder Duplikate der Daten werden ohne Wissen und Zustimmung des Auftraggebers nicht erstellt.

Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach durch dokumentierte Weisungen geändert, ergänzt oder ersetzt werden.

Weisungsberechtigte Personen des Auftraggebers sind:
Zu benennen

Weisungsempfänger beim Auftragnehmer sind:
Constantin Schünemann und Moritz Ten Eikelder

Der AN verarbeitet die personenbezogenen Daten auf keine andere Weise und für keine anderen Zwecke, sofern er nicht hierzu gesetzlich verpflichtet ist

(3) Sind personenbezogene Daten zu berichtigen, zu löschen oder zu sperren, nimmt dies der AN in angemessener Zeit vor, und wird dies dem AG schriftlich bestätigen.

(4) Die Parteien verpflichten sich einen Datenschutzbeauftragten zu bestellen, soweit dies gesetzlich vorgeschrieben ist, dessen Kontaktdaten mitzuteilen und mit dem Datenschutzbeauftragten des Auftraggebers zusammenzuarbeiten

Datenschutzbeauftragte/r des AG: (falls vorhanden oder notwendig ausfüllen)

Externer Datenschutzbeauftragte/r des AN:
heyData UG (haftungsbeschränkt), Daniel Deutsch,
Telefon +49 89 41325320, E-Mail: datenschutz@heydata.de

(5) Der AN wird seine Beschäftigten, die mit der Verarbeitung personenbezogener Daten betraut sind, mit den maßgebenden Bestimmungen des Datenschutzes vertraut machen und sie schriftlich zur Vertraulichkeit und auf das Datengeheimnis verpflichten.

(6) Gelangen die Daten des Auftraggebers unrechtmäßig, das heißt unter Verstoß gegen anwendbares Datenschutzrecht, diesen Vertrag oder Weisungen des Auftraggebers, zur Kenntnis eines unbefugten Dritten, informiert der AN den AG hierüber unverzüglich.

(7) Unterstützungs- und Informationspflicht. Sofern der AG seinen Pflichten gegenüber den betroffenen Personen (insbesondere der Pflicht, einer betroffenen Person Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu geben), nur mit Hilfe des Auftragnehmers erfüllen kann, wird der AN den AG hierbei auf dessen Anforderung unterstützen. Der AG wird den AN nach Zeitaufwand entsprechend des eingesetzten Personals in ortsüblicher und angemessener Höhe entschädigen.

Ebenso kann der AN unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den AG nach gesonderter entgeltpflichtiger Beauftragung bei der Einhaltung von dessen Verpflichtungen hinsichtlich der Sicherheit personenbezogener Daten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) sowie einer gegebenenfalls erforderlichen Datenschutz-Folgenabschätzung und vorherigen Konsultationen unterstützen.

(8) Der AN wird seine Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technisch-organisatorische Maßnahmen zur angemessenen Sicherung der personenbezogenen Daten vor Missbrauch und Verlust treffen, die den entsprechenden datenschutzrechtlichen Bestimmungen entsprechen. Der AN wird hierzu die für diesen Auftrag erforderlichen in **Anlage 1** aufgeführten technischen und organisatorischen Maßnahmen umsetzen und einhalten. Die Maßnahmen muss der AN auf Anfrage dem AG und ggfs. Aufsichtsbehörden gegenüber nachweisen.

Die technisch-organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

1. ZUTRITTSKONTROLLE
2. ZUGANGSKONTROLLE
3.ZUGRIFFSKONTROLLE / TRENNBARKEIT
4. WEITERGABEKONTROLLE

5. EINGABEKONTROLLE / SPEICHERKONTROLLE
6. AUFTRAGSKONTROLLE
7. VERFÜGBARKEITSKONTROLLE
8. ZWECKBINDUNG
9. ORGANISATIONSKONTROLLE
10. PSEUDONYMISIERUNG

Ebenso stellt der AN sicher, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur zweckentsprechend und auf Anweisung des Auftraggebers verarbeiten, es sei denn, sie sind gesetzlich zur Verarbeitung verpflichtet.

Für den Fall, dass die beim AN getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den AG. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

(9) Der AN versichert, die Einhaltung der Verpflichtung und wird während der Laufzeit dieser Vereinbarung angemessenen Versicherungsschutz für Haftpflichtschäden vorhalten und dies auf Aufforderung dem AG nachweisen. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(10) Der AG ist berechtigt, die Einhaltung der gesetzlichen Vorschriften über den Datenschutz, die vertraglichen Vereinbarungen der Parteien und die Einhaltung der Weisungen des Auftraggebers beim AN zu kontrollieren. Der AN wird den AG zu solchen Kontrollen unterstützen und diese ermöglichen. Die Unterstützung erfolgt insbesondere durch zur Verfügungstellung aller erforderlichen Informationen zum Nachweis der Einhaltung der Datenschutzbestimmungen.

(11) Befugnis des Auftragnehmers zur Berichtigung, Löschung und Sperrung
Gesetzliche bzw. vertragliche Lösch- bzw. Speicherfristen der im Auftrag verarbeiteten Daten werden durch den AN nach eigenem Ermessen sichergestellt. Darüber hinaus darf der AN die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, datenschutzgerecht löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AN wendet, wird der AN dieses Ersuchen an den AG weiterleiten.

(12) Betroffenenrechte
Löschanspruch, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft werden durch den AN nach eigenem Ermessen sichergestellt und nach entsprechender dokumentierter Weisung des Auftraggebers im Einzelfall umgesetzt.

(13) Nach Abschluss der vertraglichen Arbeiten hat der AN nach Weisung des Auftraggebers sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen.

§ 4 Subunternehmern/ Unterauftragsverhältnisse

(1) Unterauftragsverhältnisse im Sinne der Datenverarbeitung im Auftrag
Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der AN z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Einschaltung/Beauftragung von Unterauftragnehmern
Der AG ist nur nach vorheriger Einwilligung damit einverstanden, dass der AN zur Erfüllung seiner vertraglich zu erbringenden Leistungen unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO Unterauftragnehmer zur Leistungserfüllung heranzieht. Im Falle der Einwilligung hat der AN vertraglich sicherzustellen, dass die vereinbarten Regelungen auch

gegenüber Subunternehmern gelten. Der AN hat die Einhaltung der vertraglichen Pflichten durch den Subunternehmer regelmäßig zu überprüfen.

(3) Weitergabe der Daten an den Unterauftragnehmer
Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung nach § 3 Abs. 2 des Vertrages gestattet und wenn der Subunternehmer die Verpflichtung nach § 2 Abs. 9 des Vertrages erfüllt hat.

§ 5 Schweigepflicht / Datengeheimnis

Der AN verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren und seine Mitarbeiter entsprechend zu verpflichten.

Die besondere Schweigepflicht, insbesondere die einschlägigen datenschutzrechtlichen Vorschriften gerade im Umgang mit den persönlichen Daten der Kunden des Auftraggebers und die Strafbarkeit der Verletzung der Schweigepflicht sind dem AN bekannt. Dazu hat der AN aktenkundige Belehrungen durchzuführen und seine Mitarbeiter schriftlich zur Geheimhaltung zu verpflichten und diese Erklärung auf Verlangen dem AG nachzuweisen. Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes / Schweigepflicht gem. § 203 StGB vertraut macht. Der AN überwacht die Einhaltung der vorbezeichneten Vorschriften und des allg. Datengeheimnisses.

Auskünfte an Dritte darf der AN nur nach vorheriger schriftlicher Zustimmung durch den AG erteilen.

Die Tätigkeit des Auftragnehmers ist erforderlich, damit Mitarbeitern des AG die Zusammenarbeit an internen Dokumenten erleichtert wird.

Der AN und deren Erfüllungsgehilfen sind hierdurch Mitwirkender i. S. d. § 203 Abs. 4 StGB und können wenn die Kundendaten des Auftraggebers Dritten offenbart werden mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden.

Die besondere Schweigepflicht gerade im Umgang mit den persönlichen Daten der Kunden des Auftraggebers und die Strafbarkeit der Verletzung der Schweigepflicht sind dem AN bekannt.

§ 6 Vertragslaufzeit

Der Vertrag hat eine Laufzeit von einem Jahr ab dem Tag der Unterzeichnung. Er verlängert sich jeweils zum Laufzeitende um ein weiteres Jahr, wenn er nicht vor Ablauf der jeweiligen Laufzeit unter Einhaltung einer Kündigungsfrist von drei Monaten zum Laufzeitende gekündigt wird.

Das Recht zur außerordentlichen Kündigung mit wichtigem Grund bleibt unberührt.

Spätestens mit Vertragsbeendigung wird der AN die Daten des Auftraggebers von seinen Datenträgern löschen und entsprechende Unterlagen bei sich vernichten, sofern der AN nicht gesetzlich zur weiteren Aufbewahrung verpflichtet ist oder ein berechtigtes Interesse an der Datenaufbewahrung hat.

Die vorstehenden Löschungspflichten gelten nicht für Datenkopien, die in regelmäßig erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragnehmers enthalten sind, deren isolierte Löschung für den AN einen erheblichen Aufwand bedeuten würde und die im Rahmen des vom AN angewandten.

Die Verpflichtungen des Auftragnehmers aus diesem Vertrag gelten 3 Jahre über die Beendigung des Vertrages hinaus, die Verpflichtung zur Schweigepflicht unbegrenzt.

§ 7 Haftung

Der AN und seine Erfüllungsgehilfen haften nicht für Sachschäden und Aufwendungen, die dem Aufraggeber infolge der Durchführung des Vertrages entstehen, es sei denn, dass der AN oder dessen Erfüllungsgehilfen den Schaden vorsätzlich oder grob fahrlässig herbeigeführt haben. Die Haftung für

grobe Fahrlässigkeit ist der Höhe nach auf den vertragstypischen Durchschnittsschaden beschränkt und auf die Haftpflichtversicherungssummen der Haftpflichtversicherung des Auftraggebers begrenzt.
Ein Ausschluss oder eine Begrenzung der Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung des Auftraggebers oder einer vorsätzlichen oder fahrlässigen Pflichtverletzung oder Erfüllungsgehilfen beruhen, ist damit nicht verbunden. Die Haftung des Auftragnehmers für entgangenen Gewinn des Auftraggebers wird ausgeschlossen.

§ 8 Schlussbestimmungen

(1) Nebenabreden und Änderungen des Vertrages bedürfen zu ihrer Rechtsgültigkeit der Schriftform, das gilt auch für die Änderung der Schriftformklausel.

(2) Auf den Vertrag findet deutsches Recht Anwendung. Erfüllungsort ist Berlin.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder sollte sich in dieser Vereinbarung eine Lücke herausstellen, so wird die Gültigkeit der übrigen Bestimmungen hierdurch nicht berührt. Anstelle der unwirksamen Vereinbarungsbestimmung oder zur Ausfüllung der Lücke soll eine rechtswirksame Ersatzregelung treten, die dem aus dieser Vereinbarung erkennbaren Willen der Parteien, dem wirtschaftlichen Sinn und Zweck der wegfallenden Regelung und der Gesamtvereinbarung Rechnung trägt bzw. möglichst nahe kommt.

_____	BERLIN, 22.06.2020_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragnehmer

Anlage 1: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Sicherheitsschlösser
- Sorgfältige Auswahl des Reinigungspersonals

b) Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- Authentifikation mit Benutzer + Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Verschlüsselung von Notebooks / Tablets
- Benutzerberechtigungen verwalten
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe / Passwortregeln

c) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- Einsatz von Aktenvernichtern (cross cut)
- Protokollierung der Vernichtung von Daten
- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Verwaltung der Benutzerrechte durch Systemadministratoren

d) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten
- Interne Abweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Hierzu werden die Daten vor der Weiterverarbeitung mit eindeutigen Pseudonymen verknüpft und weitere personenbezogene Daten entfernt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

b) Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- Feuerlöschgeräte in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Datenschutztresor
- Erstellen eines Backup- & Recoverykonzepts
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Keine sanitären Anlagen im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)

b) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

- Kennzeichnung optionaler Eingabefelder in Online-Formularen
- Pseudonymisierung von Daten vor der Weiterverarbeitung

d) Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten