Vertrag zur Auftragsverarbeitung

gem. Art. 28 DSGVO

Für die unter § 1 fallenden Aufgaben durch den Auftragnehmer

- nachfolgend „Leistungsvereinbarung“ -

zwischen dem

Kunden von HighX

- nachfolgend „Verantwortlicher“ -

und

HighX, den Inhabern Ringo Hollenbach, Königstraße 64, 39116 Magdeburg, Deutschland &
Paul Eix, Sonnenallee 2, 39116 Magdeburg, Deutschland

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhaltsverzeichnis

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (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 - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich und Gegenstand der Verarbeitung

(1)
Diese Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: „Verarbeitung“) sämtlicher personenbezogener Daten (im Folgenden: „Daten“), die im Rahmen der Nutzung der vom Auftragsverarbeiter bereitgestellten Leistungen erfolgen.

(2)
Der Auftragsverarbeiter stellt dem Verantwortlichen eine All-in-One-Plattform als Software-as-a-Service (SaaS) zur Verfügung und erbringt ergänzende Managed Services zur Automatisierung und Integration von Geschäftsprozessen. Dabei können personenbezogene Daten automatisiert zwischen verschiedenen Systemen übertragen, verarbeitet oder gespeichert werden.

(3)
Zur technischen Umsetzung dieser Prozesse nutzt der Auftragsverarbeiter Automatisierungs- und Integrationsplattformen. Diese fungieren hierbei als Unterauftragsverarbeiter im Sinne von Art. 28 Abs. 2 DSGVO. Die Nutzung erfolgt auf Grundlage eines gesonderten Auftragsverarbeitungsvertrags gemäß Art. 28 DSGVO zwischen dem Auftragsverarbeiter und den Anbietern.

(4)
Nicht unter den Anwendungsbereich dieser Vereinbarung fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Dauer und Konkretisierung des Auftragsinhalts

(1) Die Dauer der Verarbeitung der Daten ergibt sich aus dem bestehenden Geschäftsverhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Die Verarbeitung endet sofern der Auftraggeber die Verarbeitung einstellen lässt oder das Geschäftsverhältnis beendet wird.

(2) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragsverarbeiter Daten des Verantwortlichen verarbeitet (einschließlich Backups).

(3) Im Fall eines Widerspruchs zwischen dieser Vereinbarung und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Vertragsparteien bestehen oder später eingegangen oder geschlossen werden, hat diese Vereinbarung Vorrang.

(4) Umfang, Art und Zweck der verarbeiteten Daten durch den Auftragsverarbeiter für den Verantwortlichen lassen sich folgendermaßen beschreiben:

- Im Rahmen der Bereitstellung der Software HighX in Form von Software as a Service (SaaS) werden personenbezogene Daten von Kunden des Auftraggebers verarbeitet. Dies umfasst unter anderem Namen, Adressen, Kontaktdaten.

(5) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

- Basisinformationen: Name, Adresse, Telefonnummer, E-Mail-Adresse
- Demografische Daten: Geschlecht, Alter, Beruf, Bildungsstand
- Online-Identifikatoren: Cookies, IP-Adresse, Geräte-ID
- Verhaltensbasierte Daten: Besuchte Webseiten, Klickverhalten, Dauer des Webseitenbesuchs, Interaktion mit Inhalten und Werbung
- Transaktionsdaten: Kaufhistorie, Art und Anzahl der gekauften Produkte, Zeitpunkt und Ort des Kaufs
- Kommunikationsdaten: E-Mail-Kommunikation, Chat-Historie, Kundenbewertungen und -feedback
- Soziale Medien und externe Plattformen: Likes und Shares, Kommentare, Profilinformationen aus sozialen Netzwerken, wenn diese für Marketingzwecke verwendet werden
- Geo-Lokalisierungsdaten: Standort des Nutzers basierend auf IP-Adresse, GPS oder anderen Technologien
- Technische Daten: Betriebssystem, Browsertyp und -version, Bildschirmauflösung
- Präferenzen und Interessen: Produktinteressen, Themenvorlieben, Newsletter-Abonnements

(6) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen sind:

- Kunden des Auftraggebers
- Interessenten
- Beschäftigte des Auftraggebers
- Lieferanten des Auftraggebers
- Abonnenten

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Verlangt der Verantwortliche die Umsetzung einer Weisung, obwohl der Auftragsverarbeiter den Verantwortlichen darüber informiert hat, dass diese Weisung seiner Meinung nach gegen datenschutzrechtliche Vorschriften verstoße, so trägt alleine der Verantwortliche die daraus resultierenden rechtlichen Konsequenzen.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher Zustimmung in Textform durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt (Ausgenommen sind Backups).

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt

entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Europäischen Union statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Erfolgt eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) gewährleistet der Auftragsverarbeiter die Festlegung und Einhaltung angemessener technischer und organisatorischer Maßnahmen für die jeweilige Verarbeitungssituation.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern gesetzlich vorgeschrieben, hat der Auftragsverarbeiter eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind in diesem Fall dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme auf Anfrage mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die im Anhang 1 „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der im Anhang 1 „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere

Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch

- durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren),
- durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO,
- einer Zertifizierung nach Art. 42 DSGVO oder
- einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich im Benehmen mit dem Auftragsverarbeiter jederzeit zu Prüfzwecken in dessen Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher Zustimmung in Textform des Verantwortlichen in Anspruch nehmen. Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind im Anhang 2: “Genehmigte Unterauftragsverhältnisse” im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Sofern es sich um eine allgemeine Genehmigung in Schrift- oder Textform handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch

im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung. (3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten. (4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen (sofern benannt) sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen (sofern benannt) mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Geheimhaltung

(1) Die Vertragsparteien sind verpflichtet, die ihnen unter diesem Vertrag von der jeweils anderen Partei zugänglich gemachten Informationen sowie Kenntnisse, die sie bei dieser Zusammenarbeit über Angelegenheiten – etwa technischer, kommerzieller oder organisatorischer Art – von der jeweils anderen Vertragspartei erlangen, vertraulich zu behandeln und während der Dauer sowie nach Beendigung dieser Vereinbarung ohne die vorherige Einwilligung in Textform der betroffenen Partei nicht für andere Zwecke als die Durchführung dieser Vereinbarung zu verwerten oder zu nutzen oder Dritten zugänglich zu machen. Eine Nutzung dieser Informationen ist allein auf den Gebrauch zur Durchführung dieser Vereinbarung beschränkt.

(2) Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die

- bei Vertragsabschluss bereits allgemein bekannt waren oder
- nachträglich ohne Verstoß gegen die in dieser Vereinbarung enthaltenen Verpflichtungen allgemein bekannt wurden oder
- Gegenstand von Ermittlungen durch Behörden oder Gerichte sind und im Zuge dieser Ermittlungen aufgrund einer Verfügung oder eines Beschlusses herauszugeben sind.

§ 11 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

§ 12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer Vereinbarung in Textform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Magdeburg, 16.01.2025

Datum, Ort

Unterschrift (Verantwortlicher)

Hollenbach, Ringo, Inhaber

Name, Vorname, Funktion

Unterschrift (Verantwortlicher)

Eix, Paul, Inhaber

Name, Vorname, Funktion

Anhang 1 „Technisch-organisatorische Maßnahmen“

nach Art. 32 DSGVO

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

Konkrete Beschreibung der technisch-organisatorischen Maßnahmen des Auftragsverarbeiters unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen:

Grundlegende technische und organisatorische Maßnahmen im Rahmen der Nutzung der Cloud-Providers für die Bereitstellung der angebotenen Services werden direkt durch den jeweiligen Service-Provider erbracht.

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

1.1 Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Zutrittskontrollsystem durch Schlüssel
- Schlüsselvergabe und Schlüsselmanagement erfolgt nach einem definierten Prozess
- Zutrittsberechtigung nur für berechtigte Personen
- Abschließen von Räumen nach Arbeitsschluss
- Gäste werden innerhalb des Betriebsgeländes stets begleitet

1.2 Zugangskontrolle

Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.

- Server sind nur nach einem individuellen Login nutzbar
- Clients sind nur nach einem individuellen Login nutzbar
- Login mit Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Anweisung zum Sperren des IT-Systems bei Verlassen des Arbeitsplatzes
- Automatische Sperrung bei Pausen und Fehlanmeldungen (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware
- Verschlüsselung von Datenträgern
- mobile IT-Systeme sind verschlüsselt
- mobile Datenträger sind verschlüsselt

1.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Berechtigungen werden ausschließlich von Administratoren eingerichtet
- Anzahl der Administratoren ist weitgehend reduziert

- ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen
- Zugriffe auf Anwendungen und/oder Daten werden protokolliert und können ausgewertet werden
- nicht mehr verwendete Datenträger werden sicher gelöscht / vernichtet
- Papierunterlagen mit personenbezogenen Daten werden sicher vernichtet
- Daten-Löschungen/-Vernichtungen werden protokolliert

1.4 Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Interne Mandantenfähigkeit (z.B.: Daten von unterschiedlichen Auftraggebern sind logisch/physikalisch voneinander getrennt)
- Funktionstrennung (Produktion/Test)
- Zuständigkeiten und Verantwortlichkeiten sind eindeutig festgelegt

1.5 Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)
Ein Personenbezug ist nur möglich, wenn zusätzliche Informationen hinzugezogen werden können.

- personenbezogene Daten werden, soweit möglich, nur unter einem Pseudonym gespeichert
- die zusätzlichen Informationen, die einen Personenbezug herstellen können, werden unter Verschluss aufbewahrt

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

2.1. Weitergabekontrolle
Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, …

- Mitarbeiter in Kundenprojekten werden belehrt über die zulässige Nutzung und Weitergabe von Daten
- E-Mail-Verschlüsselung

2.2. Eingabekontrolle
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Mitarbeiter sind verpflichtet, nur unter ihren eigenen Benutzerkonten zu arbeiten
- Zugriff auf die Protokolle ist nur Berechtigten möglich

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

3.1. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Verfahren zur regelmäßigen Sicherung der Daten (Backup)
- getrennte und katastrophensichere Aufbewahrung von Backups
- Einspielen von Backups wird regelmäßig getestet (Recovery)
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, Spam-Filter)
- IT-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert
- Feuer- und Rauchmeldeanlagen sind vorhanden

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

- Beschäftigten sind zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet
- Vorgaben zum Umgang mit Datenpannen sind für Mitarbeiter vorhanden
- interne Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst
- Verzeichnis von Verarbeitungstätigkeiten im Sinn des Art. 30 DSGVO wird geführt

4.2 Incident-Response-Management

- Vorgaben vorhanden, was als Datenpanne anzusehen ist
- Vorgaben vorhanden, wie mit Datenpannen umzugehen ist

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

- Rechte- und Rollenkonzept nach dem „Need to know“-Prinzip
- externe Ressourcen werden, soweit möglich, vermieden

4.4 Auftragskontrolle

- Eindeutige Vertragsgestaltung
- formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung
- Subunternehmer werden schriftlich beauftragt

Anhang 2 „Genehmigte Unterauftragsverhältnisse“

Unterauftragsverarbeiter	Anschrift / Land	Datenverarbeitung
HighLevel Inc.	400 North Saint Paul St., Suite 920 Dallas, Texas 75201, USA	Hosting und Betrieb der Plattform, inkl. Verwaltung von Social-Media-Accounts, Content-Planung und -Veröffentlichung, Nachrichtenautomatisierung sowie zentraler Nachrichtenverwaltung
n8n	Novalisstr. 10 10115, Berlin, Deutschland	Automatisierung und Integration von Geschäftsprozessen, Verknüpfung von Drittdiensten sowie Übertragung personenbezogener Daten zwischen Systemen
OpenAI	117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Integration von Large Language Models, automatisierte Textgenerierung und Datenanalyse
Anthropic, PBC	548 Market St, PMB 90375, San Francisco, CA 94104, USA	Integration von Large Language Models, automatisierte Textgenerierung und Datenanalyse
Tavily	33 West 60th Street New York, NY 10023, USA	Automatisierte Webrecherche auf Basis von Nutzereingaben zur Generierung von Antworten
templated.io	Rua Desbravador Ceará, 478 Presidente Prudente-São Paulo 19015-190 Brazil	Automatisierte Generierung von Bild-Content auf Basis von Templates, Verarbeitung und Speicherung von Kundeninhalten wie Fotos und Texten
Qdrant	Chausseestraße 86 10115 Berlin, Deutschland	Speicherung und semantische Suche in internen Wissens- und Dokumentationsdaten mittels Vektor-Datenbank

Supabase	65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	Speicherung und Verarbeitung von Nutzerdaten, Kundendaten, Anwendungsdaten sowie Nutzungsstatistiken im Rahmen des Betriebs der Plattform
Preset Inc.	548 Market Street PMB 36579 San Francisco, CA 94104, USA	Analyse und Visualisierung von in Supabase gespeicherten Nutzungsstatistiken zur internen Auswertung und Optimierung der Dienstleistungen
Userback Pty Ltd	8/31 Queen Street Melbourne VIC 3000, Australia	Erfassung und Verarbeitung von Nutzerfeedback, Fehlermeldungen sowie Übermittlung von Screenshots und Bildschirmaufzeichnungen zur Analyse und Optimierung von Website und Services
Slack Technologies, LLC	500 Howard Street San Francisco, CA 94105, USA	Interne und externe Kommunikation, Austausch von Nachrichten und Dateien sowie Organisation von Projekten und Teamzusammenarbeit
Vercel Inc.	440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting und Bereitstellung von Webanwendungen, inkl. Verarbeitung technischer Zugriffsdaten
Shotstack Pty Ltd	1/69 Broome Street, Maroubra, NSW 2035, Australia	Cloud-basiertes Video-Rendering, automatisierte Verarbeitung und Bereitstellung von Videos