VERTRAG

ZUR VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG

zwischen

_____
(Firmenname)

_____
(Adresse)

_____
(PLZ Ort)

_____
(Land)

("**Verantwortlicher** ")

und

FINDOLOGIC GmbH
Jakob-Haringer-Str. 5a
5020 Salzburg
Österreich

("**Auftragsverarbeiter**")

1. PRÄAMBEL

Der Auftragsverarbeiter erbringt gegenüber dem Verantwortlichen im Rahmen eines gesonderten Vertrages und / oder auf Grundlage gesonderter Einzelaufträge (im Folgenden insgesamt als "Hauptvertrag" bezeichnet) verschiedene Dienstleistungen im Bereich Suche, Navigation, Personalisierung und Merchandising im Kontext der Webseite des Verantwortlichen (im Folgenden insgesamt als "Leistungen" bezeichnet). Die Leistungen sind im Hauptvertrag und den jeweiligen Leistungsbeschreibungen näher beschrieben.

2. GEGENSTAND

2.1. Verarbeitung personenbezogener Daten

Diese Vereinbarung ("Vertrag") regelt die Verarbeitung von personenbezogenen Daten, welche der Auftragsverarbeiter im Rahmen der Erbringung der Leistungen für den Verantwortlichen verarbeitet ("Daten") und ist als Ergänzung zum Hauptvertrag zwischen Verantwortlichem und Auftragsverarbeiter zu verstehen.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Daten umfassen insbesondere die IP-Adresse und Browser-Identifikation der Benutzer der Webseite des Verantwortlichen und damit verknüpfte, auf die erbrachten Leistungen bezogene Verhaltensdaten wie Suchanfragen, besuchte Kategorien, ausgewählte Filter sowie angeschaute und gekaufte Produkte.

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Besucher der Webseite des Verantwortlichen

Die Verarbeitung der personenbezogenen Daten erfolgt durch erfassen, speichern, verarbeiten und löschen.

Das im Zuge der Auftragsverarbeitung zur Kenntnis gelangte personenbezogene Datum (IP-Adresse) wird zu Verrechnungszwecken für die Dauer von 6 (Sechs) Monaten verarbeitet, nach diesem Zeitraum wird dieses anonymisiert. Sofern es jedoch entsprechend gesetzlicher Aufbewahrungs- und Dokumentationspflichten, bzw. bis zur Beendigung eines allfälligen Rechtsstreits, etc., erforderlich ist, wird das personenbezogene Datum darüber hinaus verarbeitet.

2.2. Inhalt der Auftragsverarbeitung

Gegenstand, Dauer, Art und Zweck der Verarbeitung der Daten ergeben sich aus dem Hauptvertrag und den jeweiligen Leistungsbeschreibungen.

3. PFLICHTEN DES VERANTWORTLICHEN

3.1. Weisungen

Soweit die Datenverarbeitung durch den Auftragsverarbeiter im Rahmen einer dem Verantwortlichen zur Online-Nutzung zur Verfügung gestellten Standard-Software erfolgt, übt der Verantwortliche sein Weisungsrecht (siehe Ziffer 4.1) in der Regel durch die eigene Benutzung der Online-Schnittstelle dieser Software aus. Im Übrigen sind Weisungen des Verantwortlichen entweder über die dem Verantwortlichen vom Auftragsverarbeiter zur Verfügung gestellte Web-Oberfläche oder in Textform zu erteilen; mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Dem Verantwortlichen bleiben solche Weisungen jederzeit vorbehalten. Geht der Inhalt von Weisungen des Verantwortlichen über dasjenige hinaus, was der Auftragsverarbeiter dem Verantwortlichen nach dem Hauptvertrag schuldet, hat der Verantwortliche die entsprechenden Leistungen dem Auftragsverarbeiter gesondert zu vergüten. Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht dem Auftragsverarbeiter ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

3.2. Meldepflicht

Gelangen im Verantwortungsbereich des Verantwortlichen die vom Auftragsverarbeiter gemäß dieser Vereinbarung verarbeiteten Daten des Verantwortlichen ungeplant zur Kenntnis eines unbefugten Dritten, informiert der Verantwortliche den Auftragsverarbeiter hierüber unverzüglich.

3.3. Haftung und Schadenersatz

Verantwortlicher und Auftragsverarbeiter haften gegenüber den betroffenen Personen grundsätzlich entsprechend der in Artikel 82 DSGVO getroffenen Regelungen. Die in den AGB enthaltene Haftungsbeschränkung entfaltet ihre Wirkung im Innenverhältnis.

4. PFLICHTEN DES AUFTRAGSVERARBEITERS

4.1. Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Rahmen und zum Zwecke der Erbringung der Leistungen für den Verantwortlichen und nach dessen dokumentierten Weisungen. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten auf keine andere Weise und für keine anderen Zwecke, sofern er nicht durch das Recht der EU oder der EU-Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; 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.

4.2. Hinweispflicht

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragsverarbeiter ist berechtigt die Durchführung der entsprechenden Weisung solange auszusetzen bis diese durch den Verantwortlichen bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht für den Auftragsverarbeiter nicht.

4.3. Berichtigung, Löschung und Sperrung

Sind personenbezogene Daten zu berichtigen, zu löschen oder zu sperren nimmt dies der Verantwortliche durch Nutzung der entsprechenden Funktionen der bereitgestellten Software selbst vor. Ist dies nicht möglich, übernimmt der Auftragsverarbeiter die Berichtigung, Löschung oder Sperrung gemäß den Weisungen des Verantwortlichen. Für die Löschung der Daten am Ende der Vertragslaufzeit gilt Ziffer 7.2.

4.4. Ort der Datenverarbeitung

Datenverarbeitungstätigkeiten werden zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in den USA. Das angemessene Datenschutzniveau ergibt sich aus

- einem Angemessenheitsbeschluss der Europäischen Kommission (EU-US Privacy Shield) gemäß Artikel 45 DSGVO sowie
- Standarddatenschutzklauseln gemäß Artikel 46 DSGVO

Die hinzugezogenen Sub-Auftragsverarbeiter und deren Herkunftsländer werden in Anlage 2 aufgeführt. Für Sub-Auftragsverarbeiter gelten weiterhin die Bestimmungen in Absatz 6.

4.5. Datenschutzkoordinator

Der Datenschutzkoordinator kann unter privacy@findologic.com erreicht werden.

4.6. Datengeheimnis

Der Auftragsverarbeiter 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 zur Datengeheimhaltung verpflichten. Insbesondere gilt diese Verschwiegenheitspflicht der mit der Verarbeitung der Daten betrauten Personen auch für die Daten von juristischen

Personen oder Personenvereinigungen und bleibt auch nach der Beendigung ihrer Tätigkeit für den Auftragsverarbeiter bestehen.

4.7. Meldepflicht

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten entsprechend Art. 4 Abs. 12 DSGVO, informiert der Auftragsverarbeiter den Verantwortlichen hierüber unverzüglich.

Meldungen gemäß Artikel 33 oder 34 DSGVO darf der Auftragsverarbeiter für den Verantwortlichen nur nach vorheriger Weisung des Verantwortlichen durchführen.

4.8. Unterstützungspflicht

Sofern der Verantwortliche 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 Auftragsverarbeiters erfüllen kann, wird der Auftragsverarbeiter den Verantwortlichen hierbei auf dessen Aufforderung angemessen unterstützen. Wird eine entsprechende Auskunftsanfrage an den Auftragsverarbeiter gerichtet und lässt diese erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm beanstandeten Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.

Ebenso unterstützt der Auftragsverarbeiter, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Verantwortlichen auf Anforderung 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 ggf. erforderlichen Datenschutz-Folgenabschätzung und vorherigen Konsultationen. Den entstehenden Aufwand hat der Verantwortliche dem Auftragsverarbeiter gesondert zu vergüten.

4.9. Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter alle erforderlichen technischen und organisatorischen Maßnahmen, die geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragsverarbeiter trifft in seinem Verantwortungsbereich insbesondere die in der Anlage 1 zu diesem Vertrag genannten technischen und organisatorischen Maßnahmen zum Schutz der Daten. Ebenso unternimmt der Auftragsverarbeiter Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf

Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der EU oder der EU-Mitgliedstaaten zur Verarbeitung verpflichtet.

Aufgrund der ständigen Weiterentwicklung der technischen und organisatorischen Maßnahmen ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, wobei das Sicherheitsniveau der bereits festgesetzten Maßnahmen nicht unterschritten werden darf. Wesentliche Änderungen sind zu dokumentieren und werden unmittelbar nach Vornahme der Änderung dem Verantwortlichen mitgeteilt.

Gemäß Art. 32 Abs. 1 lit. d DSGVO hat der Auftragsverarbeiter bei gegebenem Anlass, mindestens aber einmal im Jahr, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen.

4.10. Verarbeitungsverzeichnis

Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis gemäß Artikel 30 DSGVO zu errichten.

5. KONTROLLRECHTE DES VERANTWORTLICHEN

5.1. Kontrollen

Der Verantwortliche ist berechtigt, die Einhaltung a) der gesetzlichen Vorschriften über den Datenschutz, b) der vertraglichen Vereinbarungen der Parteien und c) der Weisungen des Verantwortlichen im erforderlichen Umfang beim Auftragsverarbeiter zu kontrollieren oder durch einen vom Verantwortlichen beauftragten Prüfer kontrollieren zu lassen. Der Auftragsverarbeiter wird zu solchen Kontrollen beitragen und alle erforderlichen Informationen zum Nachweis der Einhaltung zur Verfügung stellen. Kontrollen in den Betriebsstätten des Auftragsverarbeiters muss der Verantwortliche mindestens 2 (zwei) Wochen vorher schriftlich ankündigen.

Der Auftragsverarbeiter gestattet und ermöglicht dem Verantwortlichen und von ihm beauftragten Prüfern entsprechende Überprüfungen – einschließlich Inspektionen – grds. 2 (zwei) Mal im Jahr im Rahmen der üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs des Auftragsverarbeiters durchzuführen und trägt in zweckmäßigem Maße dazu bei.

5.2. Kosten

Durch Kontrollen des Verantwortlichen entstehende Kosten beim Auftragsverarbeiter trägt der Verantwortliche. Dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragsverarbeiter beanspruchten Personals.

5.3. Schutzwürdige Interessen des Auftragsverarbeiters

Soweit durch Kontrollen Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters offenbart oder geistiges Eigentum des Auftragsverarbeiters gefährdet werden kann, hat der Verantwortliche die Kontrollen auf eigene Kosten durch einen fachkundigen und unabhängigen Dritten vornehmen zu lassen, der sich gegenüber dem Auftragsverarbeiter zur Verschwiegenheit verpflichtet.

6. Sub-Auftragsverarbeiter

6.1 Genehmigte Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt die in der Anlage 2 genannten Sub-Auftragsverarbeiter hinzuzuziehen. Der Auftragsverarbeiter hat mit den Sub-Auftragsverarbeitern bereits die erforderlichen Verträge im Sinne des Art 28 Abs. 4 DSGVO abgeschossen, deren Schutzniveau mindestens demjenigen dieses Vertrages entsprechen und die den Sub-Auftragsverarbeitern dieselben Verpflichtungen auferlegen, die dem Auftragsverarbeiter auf Grund dieses Vertrages obliegen. Der Verantwortliche stimmt diesen ausdrücklich zu.

6.2. Information über beabsichtigte Änderungen

Der Auftragsverarbeiter ist zudem befugt, weitere Sub-Auftragsverarbeiter hinzuzuziehen. Der Auftragsverarbeiter hat den Verantwortlichen von der beabsichtigten Hinzuziehung eines weiteren Sub-Auftragsverarbeiters zu verständigen. Der Verantwortliche kann diesfalls binnen 4 Wochen in Textform berechtigte Einwendungen erheben. Tut er dies nicht, gilt die Zustimmung des Verantwortlichen als erteilt.

Der Auftragsverarbeiter schließt mit dem Sub-Auftragsverarbeiter einen erforderlichen Vertrag im Sinne des Art 28 Abs. 4 DSGVO ab. Der Auftragsverarbeiter stellt sicher, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieses Vertrages obliegen.

6.3. Sub-Auftragsverarbeiter in Drittstaaten

Eine Beauftragung von Subunternehmen in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, genehmigte Verhaltensregeln).

Für Sub-Auftragsverarbeiter gelten weiterhin die Bestimmungen in Absatz 4.4.

7. LAUFZEIT

7.1. Laufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

7.2. Daten bei Vertragsende

Bis längstens 6 (sechs) Monaten nach dem Ablauf / der Aufkündigung des Hauptvertrags – womit dieser Vertrag ebenfalls als abgelaufen / aufgekündigt gilt – wird der Auftragsverarbeiter die im Rahmen der Erbringung seiner Leistungen für den Verantwortlichen verarbeiteten personenbezogenen Daten in dessen Auftrag von seinen Datenträgern löschen und entsprechende Unterlagen bei sich vernichten, sofern der Auftragsverarbeiter nicht gesetzlich zur weiteren Aufbewahrung verpflichtet ist. Der Verantwortliche ist selbst dafür verantwortlich, Daten rechtzeitig vor Ablauf dieser Frist zu exportieren und zur weiteren eigenen Verwendung zu sichern. Eine Herausgabe oder ein Export von Daten, der nicht über die im Rahmen der Leistungen enthaltenen Standardfunktionen möglich ist (z.B. Download von Dateien), hat der Verantwortliche rechtzeitig gesondert zu beauftragen und zu vergüten.

7.3. Sicherungskopien

Die vorstehenden Löschungspflichten gelten nicht für Datenkopien, die in regelmäßig erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragsverarbeiters enthalten sind, deren isolierte Löschung für den Auftragsverarbeiter einen erheblichen Aufwand bedeuten würde und die im Rahmen des vom Auftragsverarbeiter angewandten Sicherungs-Zyklus spätestens nach 6 (sechs) Monaten automatisch gelöscht oder ersetzt werden. Die Wiederherstellung und jede sonstige Nutzung solcher Kopien bis zu ihrer automatischen Löschung bzw. Überschreibung ist nach Vertragsbeendigung unzulässig.

Der Verantwortliche kann vom Auftragsverarbeiter auch die sofortige Löschung solcher Sicherungskopien verlangen, wenn der Verantwortliche dem Auftragsverarbeiter die hierdurch verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragsverarbeiter beanspruchten Personals.

8. SCHLUSSBESTIMMUNGEN

8.1. Anwendbares Recht

Soweit sich nicht aus dem Hauptvertrag eine andere Rechtswahl ergibt, findet auf diesen Vertrag ausschließlich österreichisches Recht Anwendung (ohne eventuelle Verweisungen auf andere Rechtsordnungen und unter Ausschluss des UN Kaufrechts).

8.2. Gerichtsstand

Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag Salzburg, Österreich.

8.3. Teilunwirksamkeit

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Statt der unwirksamen Bestimmung gilt dasjenige, was die Parteien nach dem ursprünglich angestrebten Zweck unter wirtschaftlicher Betrachtungsweise redlicherweise vereinbart hätten. Das Gleiche gilt im Falle einer Vertragslücke.

8.4. Schriftform

Alle Änderungen und Ergänzungen zu diesem Vertrag, einschließlich etwaiger Zusicherungen des Auftragsverarbeiters bedürfen zur Gültigkeit der Schriftform, die auch in einem elektronischen Format erfolgen kann; dies gilt auch für den Fall des Abweichens von diesem Formerfordernis.

Für den **Verantwortlichen**:	Für den **Auftragsverarbeiter**:
	Matthias Heimbeck
_____	_____
Name (in Blockbuchstaben)	Name (in Blockbuchstaben)
	CEO
_____	_____
Position / Funktion	Position / Funktion
	Salzburg, 16. September 2020
_____	_____
Ort, Datum	Ort, Datum
	
_____	_____
Unterschrift	Unterschrift

ANLAGE 1: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. ZUTRITTSKONTROLLE

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Eine Verarbeitung personenbezogener Daten in den Räumlichkeiten des Auftragsverarbeiters findet nur in Ausnahmefällen wie Wartungen oder Inspektionen statt. In dieser Zeit sind die Datenverarbeitungsanlagen in ständiger Benutzung. Erweiterte Maßnahmen für Zutrittskontrollen sind daher nicht vorgesehen.

Weitere Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, werden ausschließlich durch die in Anlage 2 genannten Sub-Auftragsverarbeiter betrieben. Die Verantwortung, angemessene Zutrittskontrollen zu implementieren, liegt beim jeweiligen Sub-Auftragsverarbeiter.

2. ZUGANGSKONTROLLE

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (einschließlich Verschlüsselungsverfahren):

- Zugangsschutz (Authentisierung):
    - Es besteht Zugangsschutz zu allen Datenverarbeitungssystemen durch Benutzer-Authentisierung.
    - Die Passwörter müssen den Richtlinien im IT-Sicherheitshandbuch der Wirtschaftskammer Österreich in der 9. Auflage genügen.
- Gesicherte Übertragung von Authentisierungs-Geheimnissen (Credentials) im Netzwerk:
    - Die Übertragung der Authentisierungs-Geheimnisse über das Netz erfolgt verschlüsselt.
- Festlegung befugter Personen:
    - Es existiert – soweit vom jeweiligen Datenverarbeitungssystem unterstützt – ein Rollenkonzept (vordefinierte Benutzerprofile).
    - Zugangsberechtigungen werden – soweit vom jeweiligen Datenverarbeitungssystem unterstützt – individuell (personengebunden) vergeben.
    - Der Kreis der befugten Personen ist auf das betriebsnotwendige Minimum reduziert.
- Verwaltung und Dokumentation von personengebundenen Zugangsberechtigungen:

    - Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen ist eingerichtet, beschrieben und wird angewendet.
    - Für die Vergabe von Zugangsberechtigungen ist eine verantwortliche Person benannt.
    - Es existiert eine Vertretungsregelung.
- Manuelle Zugangssperre:
    - Es existiert eine Richtlinie, Arbeitsstationen und Terminals bei vorübergehendem Verlassen des Arbeitsplatzes gegen unbefugte Nutzung zu schützen, z.B. durch automatische oder manuelle Aktivierung des kennwortgeschützten Bildschirmschoners.

Die Nutzer werden über diese Vorgaben belehrt.

3. ZUGRIFFSKONTROLLE

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (einschließlich Verschlüsselungsverfahren):

- Berechtigungskonzept / Umsetzung von Zugriffsbeschränkungen:
    - Es gibt Regelungen zum Anlegen, Ändern und Löschen von Berechtigungsprofilen.
    - Jeder Zugangsberechtigte kann nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen:
    - Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen ist implementiert.
    - Berechtigungen sind – soweit vom jeweiligen Datenverarbeitungssystem unterstützt – an eine persönliche Benutzerkennung und an einen Account geknüpft.
    - Entfällt die Grundlage für eine Berechtigung (z.B. durch Funktionsänderung), wird diese zeitnah entzogen.
- Protokollierung des Datenzugriffs:
    - Alle Lese-, Eingabe-, Änderungs- und Löschungstransaktionen werden – soweit vom Datenverarbeitungssystem unterstützt – protokolliert.
    - Zur Missbrauchserkennung werden bei Bedarf stichprobenartige Auswertungen vorgenommen.

4. WEITERGABEKONTROLLE

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können und, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (einschließlich Verschlüsselungsverfahren):

- Sichere Datenübertragung zwischen Server und Client:
  - Die Datenübertragung zwischen Clients und Servern erfolgt verschlüsselt (SSL, SSH, SFTP oder VPN).
- Übertragung im Backend:
  - Die Verbindung zu den Backendsystemen ist geschützt.
  - Daten mit hohem Schutzbedarf werden verschlüsselt.
- Mensch-Maschine-Authentisierung:
  - Gegenseitige Authentisierung mittels kryptographischen Verfahren.
- Prozess zur Sammlung und Entsorgung:
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Datenträgern.
  - Es existieren Regelungen zur datenschutzkonformen Vernichtung von Dokumenten.
- Datenschutzgerechtes Lösch- / Zerstörungsverfahren:
  - Datenträger werden vor Wiederbenutzung durch andere Nutzer datenschutzgerecht gelöscht; eine Wiederherstellung der gelöschten Daten ist gar nicht oder nur mit unverhältnismäßigen Aufwand möglich.
  - Hardwarekomponenten oder Dokumente werden so vernichtet, dass eine Wiederherstellung gar nicht oder nur mit unverhältnismäßigen Aufwand möglich ist.

5. EINGABEKONTROLLE

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

- Es existiert eine Dokumentation darüber, welche Personen aufgrund ihrer Aufgabenstellung befugt und verantwortlich sind, personenbezogene Daten in der Datenverarbeitungsanlage einzugeben, zu verändern oder zu entfernen.

6. AUFTRAGSKONTROLLE

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle):

- Ausübung der Kontrollpflichten:
  - Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Ausübung seiner Kontrollpflichten.
  - Alle auftretenden Vorfälle werden dem Verantwortlichen gemeldet.
  - Der Auftragsverarbeiter hat alle Mitarbeiter über die Meldepflicht von Vorfällen informiert.

7. VERFÜGBARKEITSKONTROLLE

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):

- Backup-Konzept:
  - Es existiert ein Backup-Konzept.
  - Backups finden regelmäßig statt.
  - Eine für das Backup verantwortliche Person und Vertreter sind benannt.
  - Es wird regelmäßig überprüft, ob das Wiederherstellen eines Backups möglich ist.
- Prüfung der Infrastruktur:
  - Es findet eine permanente Überwachung der Betriebsparameter statt.

8. ORGANISATIONSKONTROLLE

- Prozessdefinition / -kontrolle:
  - Es gibt Verfahrensanweisungen.
  - Für die Verarbeitung von Daten im Unternehmen sind Prozesse und Arbeitsabläufe definiert.
  - Die Umsetzung und Einhaltung der Prozesse wird kontrolliert.
- Schulung / Verpflichtung:
  - Grundsätze des Datenschutzes, einschließlich technisch-organisatorischer Maßnahmen.
  - Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich den Vorgängen des Verantwortlichen (§11 UWG).
  - Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen.
  - Die Schulungen sind dokumentiert.
  - Die Schulungen werden regelmäßig wiederholt, mindestens jedoch alle drei Jahre.
- Schulung / Verpflichtung Betriebsfremder:

    - Firmenfremde erhalten erst dann Zugang zu Datenverarbeitungsanlagen, wenn diese schriftlich auf das Daten- und ggf. auch auf das Fernmeldegeheimnis bzw. weitere Verschwiegenheitsverpflichtungen verpflichtet und geschult wurden, bevor diese die Datenverarbeitungsanlagen in Betrieb nehmen und bedienen dürfen.
- Interne Aufgabenverteilung:
    - Eine Trennung zwischen operativen und administrativen Funktionen ist erfolgt.
- Vertreterregelung:
    - Für alle betriebsnotwendigen Aufgaben/Funktionen ist ein Vertreter festgelegt.

ANLAGE 2: Sub-Auftragsverarbeiter

Sub-Auftragsverarbeiter	**Vom Sub-Auftragsverarbeiter erbrachte Leistungen**	**Gewährleistung des Datenschutzniveaus**
CDN77 / DataCamp Limited 207 Regent Street London UK	Hosting von Web Assets	ADV
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting der Infrastruktur	ADV
OVH 2 Rue Kellermann 59100 Roubaix Frankreich	Hosting von Web Assets	ADV
Sentry 132 Hawthorne St San Francisco CA 94107 USA	Real-Time Error Tracking	Standardvertragsklauseln
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Hosting der Infrastruktur in der Google Cloud Platform (GCP)	Standardvertragsklauseln