AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

abgeschlossen am untenstehenden Tage zwischen der unten ausgewiesenen
„Auftraggeberin“
einerseits, und der
„Auftragnehmerin“
Captcha GmbH, Muthgasse 2, 1190 Wien
andererseits, wie folgt:

1. Präambel

1.1. Die Auftragnehmerin erbringt auf der Grundlage eines „Servicevertrages“ Dienstleistungen für die Auftraggeberin. Dabei verarbeitet die Auftragnehmerin „personenbezogene Daten“ im Sinne des Art 4 Z 1 Datenschutz-Grundverordnung (DSGVO) für die Auftraggeberin.

1.2. Diese Vereinbarung soll die vertragliche Basis für die Auftragsdatenverarbeitung im Sinne des Artikels 28 Absatz 3 DSGVO bilden und in Ergänzung des „Servicevertrages“ die Verpflichtungen der Parteien im Hinblick auf die Auftragsdatenverarbeitung verbindlich darlegen.

1.3. Diese Vereinbarung ergänzt den Servicevertrag, geht diesem ausschließlich zur Erfüllung der regulatorischen Voraussetzungen im Bereich des Datenschutzes und der Datensicherheit vor und ist geltungserhaltend im Sinne der DSGVO und der begleitenden Datenschutzgesetze auszulegen.

2. Definitionen

2.1. „Servicevertrag“: Der Provider stellt dem Kunden den Online-Zugriff auf eine CAPTCHA-Softwarelösung (Completely Automated Public Turing Test to tell Computers and Humans Apart) in Form einer Software-as-a-Service-Lösung (SaaS) zur Verfügung. Dabei handelt es sich um einen Sicherheitsmechanismus, der auch als Challenge-Response-Authentifizierung bekannt ist.

2.2. „Zweck des Servicevertrages“ (Kurzbeschreibung): Hosting, Betrieb, Wartung, kontinuierliche Verbesserung und Support der CAPTCHA-Software.

2.3. „Art der personenbezogene Daten“: Die personenbezogenen Daten, auf die der Auftragnehmerin Zugriff gewährt wird, sind in der Beilage ./1 näher definiert.

2.4. „Kategorien betroffener Personen“:
Websitenutzer

2.5. Verarbeitungsverzeichnis: Die Vertragsparteien nehmen zur Kenntnis, dass sie gemäß Art 30 Abs 1 und 2 DSGVO zur Führung eines (Auftragsdaten-) Verarbeitungsverzeichnisses verpflichtet sind.

3. Vertragsgegenstand des AVV

3.1. Diese Vereinbarung umfasst und dient dem Schutz sämtlicher personenbezogener Daten (Art 4 Z 1 DSGVO),

- die die Auftragnehmerin für die Auftraggeberin in Erfüllung ihrer vertraglichen Verpflichtungen aus dem Servicevertrag verarbeitet oder
- auf die die Auftragnehmerin Zugriff nimmt oder nehmen kann,

auch wenn sie nicht ausdrücklich in der Beilage ./1 angeführt sind.

4. Rechte und Pflichten der Auftraggeberin

4.1. Die Auftraggeberin erklärt ausdrücklich, für die vertragsgegenständlichen personenbezogenen Daten „Verantwortlicher“ im Sinne des Art 4 Z 7 DSGVO zu sein. Alleine die Auftraggeberin soll daher im Rahmen des Vertragsverhältnisses der Vertragsparteien über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheiden.

4.2. Als Verantwortlicher ist die Auftraggeberin verpflichtet, für die Zulässigkeit der Verarbeitung der personenbezoge-

nen Daten für ihre Zwecke, für die Einhaltung der DSGVO und der begleitenden Datenschutzgesetze und die Gewährung der Betroffenenrechte zu sorgen.

4.3. Deshalb steht der Auftraggeberin auch ein datenschutzrechtliches Weisungsrecht zu, in welcher Form und in welchem Umfang die personenbezogenen Daten von der Auftragnehmerin zu verarbeiten sind; sofern Weisungen der Auftraggeberin gegen das Datenschutzrecht verstoßen, so trifft die Auftragnehmerin eine Warnpflicht (Art 28 Abs 3 3. Satz DSGVO). Offensichtlich rechtswidrige Weisungen sind von der Auftragnehmerin nicht zu befolgen.

4.4. Alleine die Auftraggeberin ist daher berechtigt, über die Verwendung, Löschung und Berichtigung von personenbezogenen Daten zu entscheiden.

5. Art und Umfang der Datenverarbeitung

5.1. Die personenbezogenen Daten sind von der Auftragnehmerin

a) ausschließlich zum Zwecke der Erfüllung der vertraglichen Verpflichtungen gegenüber der Auftraggeberin zu verwenden;

b) nicht für eigene oder fremde Zwecke zu verwenden;

c) ausschließlich der Auftraggeberin zurückzugeben und nur nach schriftlichem Auftrag an Dritte zu übermitteln;

d) innerhalb des räumlichen Geltungsbereiches der DSGVO zu verarbeiten, sofern die Auftraggeberin der Verarbeitung außerhalb nicht ausdrücklich schriftlich zustimmt;

e) so zu verarbeiten, dass die Auftraggeberin jederzeit in der Lage ist, ihre datenschutzrechtlichen Pflichten gegenüber Betroffenen und Datenschutzbehörden zu erfüllen.

5.2. Jeglicher Verstoß gegen die Art und den Umfang der Datenverarbeitung durch die Auftragnehmerin führt dazu, dass sie selbst als Verantwortlicher für die unrechtmäßige Datenverarbeitung einzustehen hat (Art 28 Abs 10 DSGVO).

6. Pflichten der Auftragnehmerin

6.1. Die Auftragnehmerin ist im Umfang der übernommenen vertraglichen Verpflichtungen für die ordnungsgemäße Auftragsdatenverarbeitung im Rahmen des Servicevertrages und der bestehenden Datenschutzgesetze verantwortlich.

6.2. Verpflichtungen, die sich nicht bereits aus dem Servicevertrag oder dem objektiven Recht ergeben, können als „Anweisungen zur Datenverarbeitung“ in einem Side-Letter zu diesem Vertrag schriftlich gesondert vereinbart werden. Diese können von der Auftraggeberin von Zeit zu Zeit angepasst werden. Die Auftragnehmerin trifft die Pflicht zur ordnungsgemäßen Dokumentation von derartigen Weisungen der Auftraggeberin (Art 28 Abs 3 lit a DSGVO).

6.3. Die Auftragnehmerin verpflichtet sich, dass sie alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen, insbesondere gesetzlichen, Verschwiegenheitsverpflichtung unterliegen (Art 28 Abs 3 lit b DSGVO). Ausdrücklich sagt die Auftragnehmerin zu, dass diese befugten Personen zu den Themen Datenschutz, Datensicherheit und Vertraulichkeit ausreichen instruiert wurden. Die Verschwiegenheitsverpflichtung hat bereits vor Aufnahme der Datenverarbeitung für die Auftraggeberin zu bestehen und auch nach Beendigung der Tätigkeit unbefristet weiterzubestehen. Die Verpflichtung zur Verschwiegenheit ist auch für Daten von juristischen Personen einzuhalten.

6.4. Die Auftragnehmerin verpflichtet sich ferner, alle gemäß Art 32 DSGVO erforderlichen technischen-organisatorischen Maßnahmen zu ergreifen, um die Sicherheit der Datenverarbeitung gewährleisten zu können (Art 28 Abs 3 lit c DSGVO; siehe Beilage ./2). Die Auftragnehmerin wird daher auf eigene Kosten alle organisatorischen und technischen Maßnahmen ergreifen, die ihres Erachtens erforderlich sind, um (i) die Sicherheit und Integrität der Datenverarbeitung zu gewährleisten, (ii) Verluste personenbezogener Daten zu verhüten, und (iii) den unbefugten Zugriff Dritter auf die personenbezogenen Daten zu verhindern. Die von der Auftragnehmerin zum Zeitpunkt der Unterzeichnung dieser Vereinbarung ergriffenen Maßnahmen sind in Beilage ./2 beschrieben und für die Auftraggeberin jederzeit einsehbar.

6.5. Die Auftragnehmerin verpflichtet sich, den Auftraggeber bei der Geltendmachung von Betroffenenrechten nach

besten Kräften zu unterstützen (Art 28 Abs 3 lit e DSGVO). Die Auftragnehmerin trägt insbesondere für die technischen und organisatorischen Voraussetzungen Vorsorge, dass die Auftraggeberin ihre Verpflichtungen zum Auskunftsrecht (Art 15 DSGVO), zum Recht auf Berichtigung (Art 16 DSGVO) und zum Recht auf Löschung („Recht auf Vergessenwerden", Art 17 DSGVO) gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann. Die Auftragnehmerin überlässt der Auftraggeberin hierfür alle notwendigen Informationen.

6.6. Die Auftragnehmerin verpflichtet sich, die Auftraggeberin bei der Einhaltung ihrer Verpflichtungen gemäß Art 32 bis 36 DSGVO (insbesondere zur Vornahme ausreichender technisch-organisatorischer Maßnahmen, zur Datenschutzfolgeabschätzung und zur Security Breach Notification) nach besten Kräften zu unterstützen (Art 28 Abs 3 lit f DSGVO).

6.7. Die Auftragnehmerin ist ferner verpflichtet, die Auftraggeberin unverzüglich von jeder Verletzung des Datenschutzes oder der Datensicherheit zu informieren, insbesondere auch im Fall behördlicher Maßnahmen oder eines Insolvenzverfahrens.

7. Einsatz von Sub-Auftragsverarbeiter (Art 28 Abs 2 und Abs 3 lit d DSGVO)

7.1. Die Auftraggeberin stimmt hiermit zu, dass der Auftragnehmer andere Auftragsverarbeiter („Subauftragsverarbeiter") zur Durchführung bestimmter Verarbeitungstätigkeiten beauftragen kann. Diesem anderen Auftragsverarbeiter hat die Auftragnehmerin im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaates dieselben Datenschutzpflichten aufzuerlegen, die in dem Servicevertrag oder diesem AVV festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung der DSGVO entspricht. Kommt dieser andere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, bleibt die Auftragnehmerin gegenüber der Auftraggeberin für die Erfüllung der Pflichten dieses anderen Auftragsverarbeiters in vollem Umfang haftbar.

7.2. Die Auftraggeberin genehmigt hiermit die Beauftragung der in Beilage ./3 genannten Subauftragsverarbeiter.

7.3. Die Auftraggeberin räumt der Auftragnehmerin die allgemeine Erlaubnis ein, andere Auftragsverarbeiter unter den in Ziff. 7.1. genannten Bedingungen einzusetzen. Die Auftragnehmerin wird die Auftraggeberin über beabsichtigte Änderungen hinsichtlich der Hinzufügung oder Ersetzung anderer Auftragsverarbeiter unterrichten und ihr die Möglichkeit geben, diesen Änderungen zu widersprechen.

8. Kontrollrechte (Art 28 Abs 3 lit h DSGVO)

Die Auftragnehmerin verpflichtet sich für den Zeitraum bis 1 Jahr nach Beendigung des Servicevertrages, der Auftraggeberin auf deren Wunsch, jedoch nicht häufiger als einmal im Jahr, die Erfüllung der Bedingungen dieser Vereinbarung nachzuweisen. Dieser Nachweis betrifft insbesondere die implementierten technischen und organisatorischen Sicherheitsmaßnahmen. Ein solcher Nachweis kann aus Bestätigungen oder Zertifizierungen interner oder externer Prüfer oder des Datenschutzbeauftragten bestehen, in besonderen Fällen auch durch Inspektionen.

9. Datenschutzbeauftragter

9.1. Bei Vorliegen der Voraussetzungen des Art 37 DSGVO ist die Auftragnehmerin (zumindest) für die Laufzeit dieser Vereinbarung verpflichtet, einen Datenschutzbeauftragten zu bestellen.

9.2. Derzeit sieht sich die Auftraggeberin nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen.

10. Vertragsdauer der AVV

10.1. Diese Vereinbarung tritt mit Zustimmung beider Vertragsparteien in Kraft und gilt für die gesamte Dauer der aufrechten Vertragsbeziehung zur Erbringung von Dienstleistung durch die Auftragnehmerin.

10.2. Die Auftragnehmerin ist nach Beendigung ihrer Dienstleistung verpflichtet, nach Weisung der Auftraggeberin alle Daten, Verarbeitungsergebnisse und Unterlagen zu retournieren oder auftragsgemäß zu löschen.

10.3. Die Verpflichtung zur Wahrung der Verschwiegenheit dauert über den Zeitraum der aufrechten Vertragsbeziehung unbefristet an.

11. Schlussbestimmungen

11.1. Änderungen und Ergänzungen zu diesem AVV bedürfen der Schriftform. Gleiches gilt für die Vereinbarung, vom Erfordernis der Schriftform abzugehen.

11.2. Diese Vereinbarung unterliegt materiellem österreichischen Recht sowie dem sachlich relevanten Unionsrecht, insbesondere der DSGVO.

11.3. Im Übrigen gelten die Regelungen des zwischen den Vertragsparteien abgeschlossenen Servicevertrages unverändert fort.

12. Beilagen

- Beilage ./1: Spezifikation der personenbezogenen Daten
- Beilage ./2: Technisch- organisatorische Maßnahmen
- Beilage ./3: Genehmigte Subunternehmer

Ort, Datum	Ort, Datum
	
Auftraggeberin / Verantwortliche	Auftragnehmerin

Beilage ./1:

Spezifikation der personenbezogenen Daten

- IP-Adresse
- Computer Model
- Browser Version
- Refer Website

Die von davon **betroffenen Personen** sind in Bezug auf den Verantwortlichen/Auftraggeber Besucher seiner Website.

Die konkrete **Verarbeitung** der Daten besteht in deren

- Erhebung/Erfassung
- Speicherung
- Organisation/Ordnung
- Anpassung/Berichtigung/Ergänzung
- Auslese
- Übermittlung/Offenlegung/Verbreitung
- Abgleich/Verknüpfung
- Einschränkung
- Löschung/Vernichtung

zu folgenden **Zwecken**

- Bereitstellung einer Challenge-Response-Authentifizierung

Beilage ./2:

Technische und organisatorische Datensicherheitsmaßnahmen

Zutrittskontrolle

- Alarmanlage / Einbruchsmeldesystem
- Videoüberwachung der Zugänge
- Zugangsbeschränkung für Büro- und Geschäftsräume
- Sicherheitsschlösser
- Schlüsselregelung
- Protokollierung von Schlüsselausgaben

Zugangskontrolle

- Sichere Aufbewahrung von Datenträgern
- „clean desk“ (digitaler Arbeitsplatz, Reinigung des virtuellen Desktop)
- Passworteingabe zur Anmeldung
- Richtlinie zur Passwortsicherheit
- Berechtigungskonzept
- Erstellung von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu Datenverarbeitungssystemen
- Authentifizierung über eindeutige User-ID
- Authentifizierung über Benutzername und Passwort
- Gesicherte Verbindung bei Fernwartung
- Protokollierung der Zugänge (An- und Abmeldung) zu kritischen Datenverarbeitungssystemen
- Kontosperre bei fehlerhaften Zugangsversuchen
- Automatische Rechnersperre bei vorübergehender Abwesenheit
- Unverzügliche Sperre der Berechtigung ausgeschiedener Benutzer
- Verwaltung der Rechte durch Systemadministrator
- Sichere Aufbewahrung des Administrator-Passworts
- Angriffserkennung/Anti-Viren-Software
- Abschottung durch Firewall
- Daten-/Festplattenverschlüsselung von mobilen Endgeräten (Blackberry, Notebook, USB-Stick etc.)
- Verbot privater Speichermedien
- Regelmäßige Aktualisierung der Schutzprogramme (Update etc.)

Zugriffskontrolle

- Zugriffsbeschränkung für Computersysteme und Netzlaufwerke auf berechtigte Benutzer
- Zugriffsbeschränkung für Backup-Datenträger auf Systemadministratoren
- Berechtigungskonzept
- Prozess zur Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen
- Berechtigungsminimierung nach Zweckbindungsprinzip
- Differenzierte Berechtigungen (Lesen, Ändern, Profile, Rollen, Objekte)
- Berechtigungsverwaltung durch Systemadministrator
- Meldung und Auswertung erfolgter/versuchter Sicherheitsverletzungen (CodeEnigma)
- Ordnungsgemäße Datenvernichtung
- Verschlüsselung von Datenträgern

Weitergabekontrolle

- Monitoring des Server-Datenverkehrs
- Verschlüsselte programmgesteuerte Übermittlung von Daten
- Kryptographische Verschlüsselungsverfahren (z.B. PGP, GPG)
- Datentransfer über gesicherte Verbindungen (z.B. https/SFTP)
- Protokollierung von Abruf- und Übermittlungsvorgängen
- Einsatz von Passwörtern und Passwortsicherheit
- Getrennte Wege zur Passwortübermittlung

Eingabekontrolle

- Nachvollziehbarkeit der Zugriffe anhand individueller Benutzernamen
- Protokollierung von Eingabe, Änderung und Löschung von Daten
- Aufbewahrung der Formulare, aus denen Daten digitalisiert wurden
- Übersicht der Applikationen, mit denen Daten eingegeben/geändert/gelöscht werden

Auftragskontrolle

- Auswahl weiterer (Sub-)Auftragnehmer nach Datensicherheitsgarantien
- Verpflichtung aller Auftragnehmer gemäß Art 28 Abs 3 DSGVO
- Sorgfältige Auswahl von IT-, Wach-, Reinigungs-, Entsorgungs-, Transport- u.a. Dienstleistern
- Sicherstellung der Rückgabe/ordnungsgemäßen Vernichtung aller Daten bei Vertragsbeendigung
- Beachtung der Voraussetzungen der DSGVO bei Auftragsdatenverarbeitung in Drittstaaten

Verfügbarkeitskontrolle

- Datensicherungskonzept
- Betriebsexterne sichere Verwahrung der Backup-Datenträger
- Führen von Backup-Verzeichnissen bzw. einer Backup-Verzeichnisstruktur
- Notfallplan/Recovery-Konzept
- Backup-Rechenzentrum (Hetzner)
- Datenwiederherstellungstests
- Einsatz spezieller Schutzprogramme
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte
- Zeitgerechte Datenverfügbarkeit und – verarbeitbarkeit
- Minimierung der Eintrittspunkte für Schadsoftware

Trennungsprinzip

- Keine Mitbenutzung der Büroräume, Archive und Server durch Fremdfirmen
- Logische Mandantentrennung
- Festlegung von Datenbankrechten (Zugriffsschranken für einzelne Ordner, Datensätze, Felder)
- Rollentrennung von Benutzern
- Berechtigungskonzept
- Verwaltung der Berechtigungen durch Systemadministrator

- Trennung von Entwicklungs- Test und Produktivsystemen

Organisation

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses
- Verpflichtung des Fremdpersonals zur Wahrung des Datengeheimnisses
- Datenschutz-Schulungen für Mitarbeiter
- Administratorkontrolle
- Löschungsregelung für Protokolldaten
- IT-Richtlinien
- Regelung privater Nutzung betrieblicher Kommunikationstechnik
- Direkt-/Adressmarketing nach datenschutzrechtlichen Vorgaben
- Einsatz von Cloud-Computing nach datenschutzrechtlichen Vorgaben
- Dokumentiertes Datenschutzkonzept

Internetauftritt / mobile Dienste

- Datenschutzerklärung
- Anbieterkennzeichnung
- Kennzeichnung kommerzieller Kommunikation/Inhalte
- Einsatz von Tracking-Software gemäß datenschutzrechtlicher Vorgaben
- Cookie-Sicherheit (HttpOnly Flag, Secure Cookie, etc.)

Beilage ./3:

Genehmigte Subunternehmer

Firma	Zweck	Übermittelte personenbezogene Daten
Krone Multimedia GesmbH & Co KG, Muthgasse 2, 1190 Wien	Techn. Entwicklung, Support/Service Dienstleistungen, Marketing, Vertrieb, Hosting	Name, Anschrift, Telefonnummer, E-Mail-Adresse, Bankdaten, Inhalte von Nachrichten des Nutzers, Inhalte von Kontaktanfragen, E-Mail Inhalte, elektronische Identifikationsdaten
Mediaprint Zeitungs- und Zeitschriftenverlag Gesellschaft m.b.H. & Co Kommanditgesellschaft, Richard Strauß Straße 16, 1230 Wien	Buchhaltung, nachgelagerte kaufmännische bzw. Finanzbezogene Verarbeitungen	Name, Anschrift, E-Mail-Adresse, Bankdaten,