1. Auftragsverarbeitungsvertrag (AVV)

Zwischen
dem im Hauptvertrag genannten Auftraggeber
– nachfolgend „Verantwortlicher“ genannt –

und
dem im Hauptvertrag genannten Auftragnehmer
– nachfolgend „Auftragsverarbeiter“ genannt –

PRÄAMBEL

Dieser Auftragsverarbeitungsvertrag (AVV) konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Zusammenhang mit den im Hauptvertrag vereinbarten Leistungen (insbesondere Betrieb und Hosting der Internetpräsenz sowie damit verbundene Supportleistungen). Er regelt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß Art. 28 DSGVO und stellt sicher, dass die Anforderungen an Datenschutz und Datensicherheit eingehalten werden.

§ 1 DEFINITIONEN

1. „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).
2. „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Art. 4 Nr. 2 DSGVO).
3. „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO).
4. „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).
5. „Unterauftragsverarbeiter“ ist jeder Auftragsverarbeiter, der im Auftrag des Hauptauftragsverarbeiters personenbezogene Daten verarbeitet.

§ 2 GEGENSTAND UND DAUER DER VERARBEITUNG

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Der genaue Gegenstand und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag zwischen den Parteien.
2. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Nach Beendigung des Hauptvertrags werden die Daten gemäß § 10 gelöscht oder zurückgegeben.

§ 3 ART UND ZWECK DER VERARBEITUNG

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu den im Hauptvertrag genannten Zwecken (Hosting, Betrieb, statistische Auswertung und Absicherung der Webseite). Eine Verarbeitung zu anderen Zwecken ist nur mit vorheriger Zustimmung des Verantwortlichen in Textform zulässig.

2. Art der verarbeiteten Daten:

    i) **Meta- und Kommunikationsdaten:** IP-Adressen (anonymisiert zur Nutzungsanalyse; vollständig zur Erkennung und Abwehr von Angriffen sowie zur Spam-Prävention für eine begrenzte Dauer von in der Regel bis zu 7 Tagen), Geräte-Informationen (z. B. Browsertyp, Betriebssystem), Zugriffszeiten und aufgerufene URLs.

3. Kategorien betroffener Personen:

    i) Besucher und Nutzer der Internetpräsenz des Auftraggebers (z. B. Kunden und Interessenten des Kiosks).

§ 4 PFLICHTEN DES AUFTRAGSVERARBEITERS

1. Der Auftragsverarbeiter verpflichtet sich, die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen zu verarbeiten.
2. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten berechtigten Personen zur Vertraulichkeit verpflichtet wurden und sich dieser bewusst sind.
3. Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen umfassen unter anderem:

    i) Pseudonymisierung und Verschlüsselung personenbezogener Daten

    ii) Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

    iii) Maßnahmen zur Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall

    iv) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

4. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit bei der Erfüllung der in den Art. 32 bis 36 DSGVO genannten Pflichten.
5. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, die zum Nachweis der Einhaltung der in diesem Vertrag festgelegten Pflichten erforderlich sind.
6. Der Auftragsverarbeiter ermöglicht und trägt zu Überprüfungen – einschließlich Inspektionen – durch den Verantwortlichen oder einen von diesem beauftragten Prüfer.
7. Der Auftragsverarbeiter dokumentiert alle Verarbeitungsaktivitäten gemäß Art. 30 Abs. 2 DSGVO.
8. Der Auftragsverarbeiter benennt einen Datenschutzbeauftragten und teilt dessen Kontaktdaten dem Verantwortlichen mit, sofern gesetzlich erforderlich.

§ 5 PFLICHTEN DES VERANTWORTLICHEN

1. Der Verantwortliche ist für die Einhaltung der gesetzlichen Datenschutzvorschriften, insbesondere der DSGVO, verantwortlich.
2. Der Verantwortliche erteilt dem Auftragsverarbeiter alle erforderlichen Weisungen zur Verarbeitung der personenbezogenen Daten.

3. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Verarbeitungsergebnisse feststellt.

§ 6 UNTERAUFTRAGSVERHÄLTNISSE

1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die derzeit eingesetzten Unterauftragsverarbeiter sind in Anlage: Liste der Unterauftragsverarbeiter aufgeführt.
2. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Zugang der Information widersprechen.
3. Der Auftragnehmer verpflichtet die Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den in diesem AVV festgelegten Pflichten entsprechen.

§ 7 RECHTE DER BETROFFENEN PERSONEN

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen, soweit möglich, bei der Erfüllung der Pflichten und Rechte der betroffenen Personen gemäß Kapitel III der DSGVO (Art. 12–23).
2. Wenn eine betroffene Person direkt an den Auftragsverarbeiter herantritt, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiter.

§ 8 MELDUNG VON DATENSCHUTZVERLETZUNGEN

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, in der Regel innerhalb von 48 Stunden nach Bekanntwerden, über alle Verletzungen des Schutzes personenbezogener Daten.
2. Die Meldung an den Verantwortlichen muss alle Informationen enthalten, die für die Erfüllung der Meldepflichten nach Art. 33 und 34 DSGVO erforderlich sind, einschließlich:
    i) Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
    ii) Kategorien und ungefähre Anzahl der betroffenen Personen
    iii) Kategorien und ungefähre Anzahl der betroffenen personenbezogenen Datensätze
    iv) Beschreibung der wahrscheinlichen Folgen der Verletzung
    v) Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Minderung ihrer möglichen nachteiligen Auswirkungen

§ 9 LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

1. Nach Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zu löschen oder zurückzugeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
2. Die Parteien vereinbaren, dass die technische Umsetzung der Rückgabe sowie die Fristen für die anschließende Löschung abschließend in den Abschnitten **Fehler! Verweisquelle konnte nicht gefunden werden.** sowie **Fehler! Verweisquelle konnte nicht gefunden werden.** des Hauptvertrages geregelt sind.
3. Der Auftragsverarbeiter bestätigt die vollständige Löschung der Daten auf Verlangen des Verantwortlichen in Textform (z. B. per E-Mail).

§ 10 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten gemäß Art. 32 DSGVO zu ergreifen. Eine Übersicht der konkreten Maßnahmen ist als Anlage: Technische und organisatorische Maßnahmen (TOM) diesem Vertrag beigefügt.

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

§ 11 AUDITRECHTE UND KONTROLLMAßNAHMEN

1. Der Verantwortliche hat das Recht, Audits durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftragsverarbeiter unterstützt den Verantwortlichen hierbei und stellt alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung.
2. Der Nachweis der Einhaltung der vereinbarten Maßnahmen erfolgt vorrangig durch die Bereitstellung aktueller Informationen, Selbstauskünfte oder Dokumentationen (z. B. die AVV und TOM der eingesetzten Subunternehmer).
3. Physische Vor-Ort-Inspektionen sind nur bei berechtigtem Anlass zulässig (z. B. bei begründetem Verdacht auf einen Datenschutzverstoß) oder wenn die Nachweise nach Absatz 2 nicht ausreichen. Solche Inspektionen sind mit einer angemessenen Frist anzukündigen, dürfen die Betriebsabläufe nicht unangemessen stören und sind in den privaten Wohnräumen des Auftragsverarbeiters ausgeschlossen.
4. Der Verantwortliche trägt die Kosten für die Durchführung eines Audits grundsätzlich selbst. Der Auftragsverarbeiter kann für einen über das übliche Maß hinausgehenden erheblichen Zusatzaufwand bei der Unterstützung eines Audits eine angemessene Aufwandsentschädigung (auf Basis des Stundensatzes gemäß § 2 des Hauptvertrages) verlangen, sofern diese vorher abgestimmt wurde.
5. Stellt das Audit einen wesentlichen Verstoß des Auftragsverarbeiters gegen datenschutzrechtliche Bestimmungen oder diesen Vertrag fest, trägt der Auftragsverarbeiter die Kosten des Audits sowie den eigenen Aufwand selbst.

§ 12 HAFTUNG

1. Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO sowie den zwingenden gesetzlichen Vorschriften.
2. Im Innenverhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter gelten die im Hauptvertrag vereinbarten Haftungsbeschränkungen und Haftungsausschlüsse, insbesondere die dort geregelte Haftungsdeckelung, auch für Ansprüche aus oder im Zusammenhang mit diesem AVV, soweit gesetzlich zulässig.

§ 13 INTERNATIONALE DATENÜBERMITTLUNGEN

1. Eine Übermittlung personenbezogener Daten in Drittländer (Länder außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums) erfolgt nur, sofern dies zur Erfüllung unserer vertraglichen Pflichten erforderlich ist, gesetzlich vorgeschrieben ist oder der Verantwortliche hierzu seine Einwilligung erteilt hat.

In jedem Fall stellt der Auftragsverarbeiter sicher, dass ein angemessenes Datenschutzniveau gewährleistet ist, beispielsweise durch:

i) Abschluss von Standardvertragsklauseln

ii) Binding Corporate Rules (BCRs)

iii) Angemessene Datenschutzvorkehrungen gemäß Art. 46 DSGVO

§ 14 SCHLUSSBESTIMMUNGEN

1. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.
2. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt die Wirksamkeit des Vertrages im Übrigen unberührt. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt diejenige wirksame und durchführbare Regelung als vereinbart, deren Wirkungen der Zielsetzung am nächsten kommen, die die Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben.
3. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Im Übrigen gelten die Schlussbestimmungen zum Gerichtsstand aus dem Hauptvertrag entsprechend.

§ 15 VERZEICHNIS DER ANLAGEN

Diesem Vertrag sind folgende Anlagen beigefügt, die als wesentliche Bestandteile der Vereinbarung anerkannt werden:

- Anlage: Liste der Unterauftragsverarbeiter
- Anlage: Technische und organisatorische Maßnahmen (TOM)

2. Anlage: Liste der Unterauftragsverarbeiter

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**	**Ort der Datenverarbeitung**
Contabo GmbH, Welfenstraße 22, 81541 München registriert im Handelsregister des Amtsgerichts München unter HRB 180722	Bereitstellung von Serverinfrastruktur (VPS/Hosting)	Deutschland / Europa
goneo Internet GmbH, Dresdener Straße 18 – 32423 Minden	Bereitstellung der E-Mail-Infrastruktur	Deutschland
Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Irland	Verwaltung des Google-Unternehmensprofils	EU (Irland)

3. Anlage: Technische und organisatorische Maßnahmen (TOM)

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

- **Zutrittskontrolle:** Die Server-Infrastruktur wird in den Rechenzentren der eingesetzten Unterauftragsverarbeiter (z. B. Contabo GmbH) betrieben, welche strenge physische Zutrittskontrollen (z. B. Alarmanlagen, Videoüberwachung) gewährleisten.
- **Zugangskontrolle:** Der Zugriff auf Server und Verwaltungsoberflächen durch den Auftragnehmer ist durch restriktive Berechtigungsverfahren, komplexe Passwörter und – soweit technisch möglich – durch Zwei-Faktor-Authentifizierung (2FA) geschützt.
- **Zugriffskontrolle:** Ausschließlich der Auftragnehmer hat administrativen Zugriff auf die Systeme. Arbeitsgeräte (Laptops) sind durch Passwort/Biometrie gesperrt.
- **Verschlüsselung:** Datenübertragungen zur Webseite erfolgen standardmäßig verschlüsselt (SSL/TLS / HTTPS).

2. Maßnahmen zur Gewährleistung der Integrität

- **Eingabe-/Weitergabekontrolle:** Nutzung abgesicherter Verbindungen (z. B. SSH/SFTP) für die Serververwaltung.

3. Maßnahmen zur Gewährleistung der Verfügbarkeit

- **Verfügbarkeitskontrolle:** Durchführung regelmäßiger Sicherungskopien (Backups) gemäß den Bestimmungen des Hauptvertrages, um eine schnelle Wiederherstellung bei Zwischenfällen zu ermöglichen. Die Rechenzentren verfügen zudem über Brandschutz- und Notstromsysteme.

4. Verfahren zur regelmäßigen Überprüfung und Evaluierung

- Regelmäßiges Einspielen von Sicherheitsupdates für Betriebssysteme, Software und eingesetzte CMS-Systeme.
- Einsatz aktueller Virenscanner und Firewalls auf den administrativen Endgeräten des Auftragnehmers.