Vereinbarung über Auftragsverarbeitungen iSd Art 28 DSGVO

abgeschlossen zwischen dem Nutzer des Cloud-Shop-Systems „Shopando“, als Verantwortlichen und der Shopando GmbH, Business Park 10 / Top 49, 8200 Gleisdorf, als Auftragsverarbeiter.

1.1

Der Auftragsverarbeiter übernimmt für den Verantwortlichen folgenden Auftrag:

Die technische Zurverfügungstellung, Verwaltung der Web-Shops des Verantwortlichen auf dem Cloud-Shop-System „Shopando“ und die softwaretechnische Abwicklung von Kaufverträgen über dieses Cloud-Shop-System. Dies beinhaltet Hosting-Leistungen für die Web-Shops des Verantwortlichen, das Management von Servern, die Bereitstellung von Storagespace, die Bereitstellung von Datenbanken und des Nutzerbereichs, die datenmäßige Verarbeitung der Nutzer-/Interessenten-/Kundendaten des Verantwortlichen, sowie zusätzliche Dienstleistungen, die in einem individuellen Vertrag festgehalten werden. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser Dienstleistungen.

Hierbei verpflichtet sich der Auftragsverarbeiter zur Geheimhaltung und zur Einhaltung der gesetzlichen Datenschutzbestimmungen gegenüber dem Verantwortlichen.

1.2

Art und Zweck der Datenverarbeitung:

Der Zweck der Datenverarbeitung liegt in der Bereitstellung der vom Verantwortlichen über das Cloud-Shop-System Shopando betriebenen Web-Shops.

1.3

Art der personenbezogenen Daten:

- Daten des Verantwortlichen: Name, E-Mail-Adresse, Firmenname, Firmenadresse, Firmenseite (URL), Log-In-Informationen, Angebotspakete und Preise des Verantwortlichen, Rechnungen an den Verantwortlichen
- Daten der Shop-Betreiber: Name, E-Mail-Adresse, Geschlecht, Firmenname, Firmenadresse, Firmenseite (URL), Log-In-Informationen der Shopbetreiber, an die der Veranwortliche Shops weiter vermietet; weiters angebotene Waren oder Dienstleistungen der Shop-Betreiber, verkaufte Waren oder Dienstleistungen an Kunden der Shop-Betreiber und für den Verkauf notwenige Daten zu diesen Waren und Dienstleitungen
- Shop-Kunden-Daten: Name, Adresse, Telefonnummer und E-Mail-Adresse der Shopkunden, wann welcher Kunde welche Waren im Shop des Shop-Betreibers gekauft hat
- Zugriffe auf das Cloud-Shop-System durch den Verantwortlichen, die Shop-Betreiber und die Shop-Kunden: Informationen über den Browsertyp und die verwendete Version, IP-Adresse des Nutzers, Datum und Uhrzeit des Zugriffs;
- Formularinhalte, Spracheinstellungen, Eingegebene Suchbegriffe, Häufigkeit von Seitenaufrufen, Inanspruchnahme von Website-Funktionen;

1.4

Kategorien betroffener Personen:

Nutzer der Web-Shops des Verantwortlichen auf dem Cloud-Shop-System Shopando; Kunden und Interessenten (Shop-Betreiber) des Verantwortlichen und deren Kunden (Shop-Kunden).

1.5

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine

internationale Organisation –, sofern er nicht durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist.

1.6
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er ohne Durchführung einer rechtlichen Prüfung durch einen Juristen der Auffassung ist, dass eine Weisung offensichtlich gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder den Mitgliedsstaaten verstößt. Der Auftragsverarbeiter ist nicht verpflichtet, sich im Zusammenhang mit der Erfüllung dieser Vereinbarung rechtlich beraten zu lassen und erbringt in Erfüllung dieser Vereinbarung auch keine Rechtsberatungsleistungen.

1.7
Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er nach dem Recht der Union oder den Mitgliedsstaaten dazu verpflichtet ist, entgegen den Weisungen des Verantwortlichen oder ohne Weisung des Verantwortlichen eine Datenverarbeitung vorzunehmen (sofern eine solche Mitteilung zulässig ist).

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

1.8
Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DSGVO zwingend erforderlichen Maßnahmen. Der Auftragsverarbeiter erfüllt seine diesbezügliche Pflicht dadurch, dass er die in Anlage 1 beschriebenen Sicherheitsmaßnahmen implementiert.

1.9
Der Auftragsverarbeiter wird den Verantwortlichen von jeder Verletzung des Schutzes personenbezogener Daten informieren, sofern dies Daten betrifft, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, und durch die Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen entsteht. Diese Information hat unverzüglich zu erfolgen, sobald der Auftragsverarbeiter von einer solchen Verletzung Kenntnis erlangt und ist an jene Kontaktstelle zu richten, die der Verantwortliche schriftlich bekannt gegeben hat.

1.10
Die unter Punkt 4.2 genannte Information des Verantwortlichen soll, soweit unter Berücksichtigung der Umstände möglich, Folgendes beinhalten:

a) die Art der Verletzung des Schutzes personenbezogener Daten, wenn möglich einschließlich der Kategorien und der ungefähren Zahl der betroffenen Personen und der Kategorien und der ungefähren Zahl der betroffenen Datensätze;
b) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten; und die vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

1.11
Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter oder Sub-Auftragsverarbeiter (im Folgenden

zusammen ”Sub-Auftragsverarbeiter"), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben und die Hinzuziehung oder die Ersetzung zu untersagen. Erhebt der Verantwortliche innerhalb von zwei Wochen keinen Einspruch, so gilt die Hinzuziehung oder Ersetzung als genehmigt.

1.12
Bei Erhebung eines Einspruchs nach Punkt 1.11 erhält der Auftragsverarbeiter das Recht, die Vereinbarung unter Wahrung einer Frist von zwei Wochen zum Monatsletzten zu kündigen.

1.13
Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des anwendbaren Datenschutzrechts erfolgt.

1.14
Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

1.15
Soweit dies möglich ist, unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß dem anwendbaren Datenschutzrecht, einschließlich Kapitel III der DSGVO.

1.16
Der Auftragsverarbeiter erfüllt seine Pflicht nach Punkt 1.15 grundsätzlich dadurch, dass er dem Verantwortlichen eingelangte Anträge von Betroffenen weiterleitet. Soweit der Verantwortliche eine zusätzliche Unterstützung des Auftragsverarbeiters für notwendig erachtet und sich der Auftragsverarbeiter dazu bereit erklärt, eine solche Unterstützungsleistung zu erbringen, ist der Auftragsverarbeiter berechtigt, hierfür eine zusätzliche angemessene Vergütung zu fordern.

1.17
Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß dem anwendbaren Datenschutzrecht, einschließlich Artikel 32-36 DSGVO. Dies erfüllt der Auftragsverarbeiter durch (a) Ergreifen der Maßnahmen unter Punkt 3 (”Vertraulichkeit") und 4 (”Datensicherheit") dieser Vereinbarung, (b) die Meldung an den Verantwortlichen über eine Verletzung des Schutzes personenbezogener Daten nach Punkt 4.2 sowie (c) durch die Zurverfügungstellung der Informationen in Anhang 1 dieser Vereinbarung.

Nach Wahl des Verantwortlichen löscht der Auftragsverarbeiter in angemessenem Zeitraum nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten oder gibt diese in angemessenem Zeitraum zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Für die Rückgabe der Daten gebührt dem Auftragsverarbeiter ein angemessenes Entgelt.

1.18
Der Auftragsverarbeiter stellt dem Verantwortlichen bei Bedarf alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung.

1.19
Der Auftragsverarbeiter ermöglicht vorangemeldete Überprüfungen zu Geschäftszeiten durch einen unabhängigen Dritten. Solche Überprüfungen werden in angemessenen zeitlichen Abständen und in einer Art durchgeführt, die den Geschäftsbetrieb des Auftragsverarbeiters nicht stören. Kosten, welche durch solche Überprüfungen anfallen, sind vom Verantwortlichen zu tragen. Dem Auftragsverarbeiter steht für alle Leistungen in Zusammenhang mit der Unterstützung von Überprüfungen ein angemessenes Entgelt zu.

1.20
Der Auftragsverarbeiter kann seine Pflichten nach Punkt 8.2 auch dadurch erfüllen, dass er zumindest alle drei Jahre eine Überprüfung durch einen unabhängigen Dritten vornehmen lässt und die zusammengefassten Prüfungsergebnisse dem Verantwortlichen zukommen lässt.

1.21
Die Haftung beider Parteien ist auf grobes Verschulden beschränkt. Eine Haftung für bloße Vermögensschäden ist ausgeschlossen.

1.22
Dessen ungeachtet haftet der Verantwortliche dem Auftragsverarbeiter für die Rechtmäßigkeit aller erteilten Weisungen und stellt ihn hinsichtlich aller aus der Befolgung einer Weisung resultierenden Schäden und Nachteile klag- und schadlos.

1.23
Die vorliegende Vereinbarung ist an etwaige geänderte Datenschutz-Bestimmungen, sofern sie für die gegenständliche Vereinbarung relevant sind, anzupassen. Sollte eine Bestimmung dieser Vereinbarung ungültig oder unwirksam sein, wird sie, soweit gesetzlich zulässig, durch jene Bestimmung ersetzt, die wirtschaftlich der ungültigen oder unwirksamen Bestimmung am nächsten kommt.

1.24
Zu dieser Vereinbarung bestehen keine mündlichen Nebenabreden. Allfällige Änderungen und Ergänzungen zu dieser Vereinbarung haben in Schriftform zu erfolgen. Dies gilt auch für die Vereinbarung des Abgehens von diesem Formerfordernis selbst.

1.25
Diese Vereinbarung unterliegt österreichischem Recht unter Ausschluss der kollisionsrechtlichen Verweisungsnormen und des UN-Kaufrechts.
Als Gerichtsstand für sämtliche Auseinandersetzungen im Zusammenhang mit dieser Vereinbarung wird das sachlich zuständige Gericht in Graz als ausschließlich zuständig vereinbart.

Anlage 1:
Technische und organisatorische Sicherheitsmaßnahmen des Auftragsverarbeiters

Anlage 1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, durch elektronische Schlüssel, Anmeldung am Empfang mit Personenkontrolle
- Zugangskontrolle: Kennwörter (einschließlich entsprechender Policy), Verschlüsselung von Datenträgern, automatische Sperrmechanismen;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten;
- Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
- Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Verschlüsselung von Datenträgern, Verschlüsselung und hashen von Passwörtern;
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch Protokollierung

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche Wiederherstellbarkeit;
- Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;