Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Anlage zu den AGB der KNISTR Loyalty App

Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen der Firma XYZ,

diejenige Firma, die die Shopify-App "KNISTR Loyalty App" über den Shopify App Store installiert hat

(im Folgenden: „**Auftraggeber**" genannt)

und der:

KNISTR GmbH
Hugh-Greene-Weg 22529 Hamburg

(im Folgenden: „**Auftragnehmer**" genannt)

Auftraggeber und Auftragnehmer gemeinsam im Folgenden: die **„Parteien"** genannt.

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3 S. 1 DSGVO)

(1) Gegenstand

Der Gegenstand des Auftrags ist die Bereitstellung und der Betrieb der Shopify Loyalty-App zur Verwaltung von Kundenbindungsprogrammen (Punktevergabe, Gutscheinsystem, Belohnungsverwaltung).

Im Rahmen der Durchführung der Leistungsvereinbarung wird der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

Nicht Gegenstand dieses Auftrags ist die Verarbeitung personenbezogener Daten, die der Auftragnehmer zu eigenen Zwecken in eigener Verantwortlichkeit durchführt, insbesondere zur

- Gewährleistung der IT-Sicherheit,
- Fehleranalyse,
- Missbrauchs- und Betrugsprävention,
- Abrechnung
- Weiterentwicklung und Verbesserung der App-Funktionalitäten.

Diese Verarbeitungen erfolgen ausschließlich ohne Nutzung personenbezogener Endkundendaten auf Basis aggregierter, anonymisierter oder statistischer Informationen. Eine Nutzung zu Marketing- oder Profilbildungszwecken findet nicht statt. Für diese Verarbeitungen ist der Auftragnehmer eigenständig Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Dauer

Die Laufzeit entspricht der Dauer der App-Installation im eigenen Shop des Händlers. Mit Deinstallation der App endet das Auftragsverhältnis automatisch, vorbehaltlich gesetzlicher Aufbewahrungspflichten.

2. Konkretisierung des Auftragsinhalts (Art. 28 Abs. 3 S. 1 DSGVO)

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung erfolgt zur Bereitstellung der Loyalty-Funktionen, insbesondere:

- Berechnung und Verwaltung von Treuepunkten,

- Verwaltung von Kundenprofilen im Loyalty-Programm,
- Erstellung und Einlösung von Belohnungen und Gutscheinen,
- technische Bereitstellung programmspezifischer Informationen.

Die Datenverarbeitung findet grundsätzlich innerhalb der Europäischen Union statt, insbesondere in der AWS-Region Frankfurt (Deutschland).

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- **Identifikations- und Profildaten:** Vorname, Nachname, E-Mail-Adresse, Shopify-Kunden-ID, Geburtstag (Tag/Monat).
- **Loyalty-Programmdaten:** Punktestand, Historie der Punktegenerierung, eingelöste Belohnungen, generierte Gutscheincodes.
- **Bestelldaten:** Bestellnummer, Bestelldatum, Kaufbetrag, gekaufte Artikel (zur Punkteberechnung), Zahlungsdetails.
- **Geräte- und Protokolldaten:** IP-Adresse, Browsertyp, Betriebssystem (zur Fehlerdiagnose und Betrugsprävention).

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen:

- Endkunden (Käufer) des Auftraggebers, die am Loyalty-Programm teilnehmen.
- Im Einzelfall Mitarbeiter und Ansprechpartner des Auftraggebers (Shop-Admins).

3. Technisch-organisatorische Maßnahmen (Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die Dokumentation der technischen und organisatorischen Maßnahmen erfolgt in der Anlage 1.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die

Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten auf Weisung (Art. 28 Abs. 3 S. 2 lit. a) DSGVO)

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, wird der Auftragnehmer den Auftraggeber in angemessenem Umfang im Zusammenhang mit Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unterstützen.

(3) Der Auftragnehmer ist berechtigt, Auskunftsansprüche betroffener Personen i.S.d. Art. 15 DSGVO für den Auftraggeber ohne erneute Konsultation zu erfüllen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Kapitel 4 der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, soweit hierzu eine gesetzliche Verpflichtung besteht bzw. Benennung eines Ansprechpartners für den Datenschutz, soweit eine solche Pflicht nicht besteht: Datenschutzanfragen können an privacy@knistr.com gerichtet werden.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b) DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die Daten des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a), 29, 32 Abs. 4 DSGVO ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO i.V.m. Anlage 1.

e) Der Auftraggeber und der Auftragnehmer arbeiten gemäß Art. 31 DSGVO auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat der Auftragnehmer ihn nach besten Kräften zu unterstützen.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. UNTERAUFTRAGSVERHÄLTNISSE (ART. 28 ABS. 2, ABS. 3 S. 2 LIT. D), ABS. 4 DSGVO)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen

angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) zur Erfüllung seiner vertraglichen Leistungspflichten einsetzen. Der Auftragnehmer informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter. Der Auftraggeber ist berechtigt, Einspruch gegen die Änderung einzulegen. Im Falle eines Einspruchs ist der Auftragnehmer zur außerordentlichen Kündigung des Hauptvertrags und dieser Vereinbarung berechtigt, wenn er durch den Einspruch in der Erbringung seiner vertraglichen Leistungspflichten beeinträchtigt wird. Die Auslagerung auf Unterauftragnehmer ist nur zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Der Auftraggeber stimmt darüber hinaus der Beauftragung der vom Auftragnehmer eingesetzten Unterauftragnehmer zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

Der Auftraggeber stimmt der Nutzung des folgenden Unterauftragnehmers zu:

Amazon Web Services (AWS) EMEA SARL (Hosting in Deutschland)

Zudem wird die **Klaviyo, Inc.,** sofern durch den Auftraggeber technisch aktiviert, als weiterer Auftragsverarbeiter des Auftraggebers eingesetzt. Der Auftragnehmer stellt in diesem Fall lediglich die technische Anbindung bereit und verarbeitet die betreffenden personenbezogenen Daten ausschließlich auf Weisung des Auftraggebers. Bei der Klaviyo, Inc. handelt es sich folglich nicht um einen Unterauftragnehmer des Auftragnehmers im Sinne dieses Vertrages.

Sofern Unterauftragnehmer ihren Sitz in einem Drittland haben, für das kein Angemessenheitsbeschluss im Sinne des Art. 45 DSGVO vorliegt, erfolgt die Datenübermittlung ausschließlich auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO (insbesondere Standardvertragsklauseln).

7. Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 S. 2 lit. h) DSGVO)

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers (Art. 28 Abs. 3 S. 2 lit. f) DSGVO)

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten des Auftraggebers unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht und Pflicht zur Wahrung von Betroffenenrechten gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers (Art. 28 Abs. 3 S. 2 lit. a), Abs. 3 S. 3 DSGVO)

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Auftrags (Art. 28 Abs. 3 S. 2 lit. g) DSGVO)

(1) Nach Deinstallation der App werden die im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten vorbehaltlich der Regelung in § 11 der AGB des Auftragnehmers innerhalb von maximal 30 Tagen gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(2) Sicherheitskopien werden entsprechend der Backup-Zyklen überschrieben.

11. Sonstiges

(1) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrerer Regelungen werden die Vertragsparteien die unwirksame Regelung durch eine solche Regelung ersetzen, die dem ursprünglichen Zweck der unwirksamen Regelung am ehesten entspricht.

(2) Soweit andere Vereinbarungen zum Zeitpunkt des Abschlusses dieses Vertrages anderslautende oder diesem Vertrag widersprechende Angaben enthalten, so gehen die Inhalte dieses Vertrages vor.

(3) Änderungen dieser Vereinbarung bedürfen der Schriftform, das gilt auch für Änderungen des Schriftformerfordernisses.

(4) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Als ausschließlicher Gerichtsstand für Ansprüche, die die Parteien im Zusammenhang mit dieser Vereinbarung geltend machen, wird Hamburg Mitte vereinbart.

(5) Diese Vereinbarung tritt mit Installation der App durch den Auftraggeber in Kraft.