VERTRAG ZUR AUFTRAGSVERARBEITUNG

nach Art. 28 DSGVO · noplastics B2B-SaaS und Shopify-App

Stand: 5. November 2026

Zwischen dem im jeweiligen Buchungs- bzw. Hauptvertrag bezeichneten Unternehmenskunden („Auftraggeber“, „Verantwortlicher“) und der NoPlastics UG (haftungsbeschränkt), Mergelweg 5, 73760 Ostfildern, vertreten durch den Geschäftsführer Marc Oliver Trautwein („Auftragnehmer“, „Auftragsverarbeiter“), wird ergänzend zum Vertrag über die Nutzung der Plattform „noplastics“ („Hauptvertrag“) dieser Vertrag vereinbart.

§ 1 Gegenstand und Verantwortlichkeiten

(1) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich in dessen Auftrag und nach dokumentierten Weisungen zur Erbringung der in Anlage 1 näher beschriebenen Leistungen. Art, Zweck, Dauer, Datenkategorien und Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Der Auftraggeber ist für die Zulässigkeit der Datenverarbeitung, die Auswahl der Daten, die Rechtsgrundlagen und die Erfüllung seiner Informationspflichten verantwortlich. noplastics ist für seine eigenen, nicht im Auftrag durchgeführten Verarbeitungen – insbesondere Vertragsverwaltung, eigene IT-Sicherheit und Abrechnung – gesondert Verantwortlicher.

(3) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag zu Fragen der Auftragsverarbeitung geht dieser AVV vor.

§ 2 Weisungen und Datenverarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Auftragsdaten nur auf dokumentierte Weisung des Auftraggebers, auch im Hinblick auf Drittlandübermittlungen, sofern nicht eine zwingende unions- oder mitgliedstaatliche Vorschrift eine abweichende Verarbeitung verlangt. Über eine solche gesetzliche Pflicht informiert der Auftragnehmer den Auftraggeber zuvor, sofern die Mitteilung rechtlich zulässig ist.

(2) Weisungen ergeben sich aus dem Hauptvertrag, diesem AVV, den App-Funktionen, Uploads, Bestätigungen, Rollen-/Freigabeentscheidungen, Veröffentlichungs-, Export- und Löschvorgängen sowie zusätzlichen Weisungen in Textform.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung Datenschutzvorschriften verletzt. Er kann deren Umsetzung bis zur Klärung aussetzen.

(4) Eine Nutzung von Auftragsdaten für eigene Werbung, die Vermarktung von Kontaktdaten oder das Training allgemeiner KI-Modelle erfolgt nicht. Von einer datenschutzrechtlich zulässigen Anonymisierung unberührte gesetzliche Pflichten bleiben bestehen.

§ 3 Besondere Verarbeitungen in der Plattform

(1) Der Auftraggeber weist noplastics an, die im gebuchten Leistungsumfang über Shopify oder Dateien übermittelten Bestell-, Versand-, Verpackungs- und Dokumentationsdaten technisch zu übernehmen, zuzuordnen, zu verarbeiten und im kundenbezogenen Workflow zu speichern. Dazu gehören gegebenenfalls in diesen Datensätzen enthaltene personenbezogene Endkundendaten.

(2) Bei automatisierter OCR-/KI-Auswertung von Dokumenten werden auch darin enthaltene Namen, Funktionen, Signaturen und Kommunikationsdaten im Auftrag verarbeitet. Ein etwaiger externer Auswertungsdienst darf personenbezogene Auftragsdaten nur nach Maßgabe der § 5 und Anlage 3 erhalten.

(3) Aktiviert der Auftraggeber Supplier Requests, weist er noplastics an, geschäftliche Kontaktpersonen in seinem Namen anzuschreiben, Antworten entgegenzunehmen und innerhalb von höchstens vier Wochen vorgesehene sachliche Erinnerungen zu versenden. Die Weisung umfasst zugehörige Kommunikationsmetadaten und Anhänge. Eine Nutzung der Lieferantenkontakte für eigene Marketingzwecke ist ausgeschlossen.

(4) Der Auftraggeber weist noplastics an, die von ihm hierfür freigegebenen Inhalte auf öffentlichen oder zugangsbeschränkten QR-/Prüfnachweisseiten bereitzustellen und zugehörige kundenbezogene Freigabe-/Audit-Metadaten zu verarbeiten. Über Umfang, Veröffentlichung und Zugangsart der Inhalte entscheidet der Auftraggeber.

(5) Nicht für den Workflow erforderliche personenbezogene Daten sind möglichst bereits vor ihrer Übermittlung auszuschließen und andernfalls ohne unangemessene Verzögerung aus dem operativen Verarbeitungsbestand zu entfernen, soweit sie nicht zur Durchführung der vereinbarten Verarbeitung benötigt werden.

§ 4 Vertraulichkeit und technische/organisatorische Maßnahmen

(1) Der Auftragnehmer stellt sicher, dass zur Auftragsverarbeitung befugte Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen.

(2) Der Auftragnehmer gewährleistet ein dem Risiko angemessenes Schutzniveau durch technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die bei Vertragsschluss vereinbarten Maßnahmen sind in Anlage 2 beschrieben. Gleichwertige oder verbesserte Maßnahmen dürfen sie ersetzen, soweit das Schutzniveau nicht abgesenkt wird.

(3) Der Auftragnehmer dokumentiert und überprüft seine Schutzmaßnahmen angemessen und stellt dem Auftraggeber auf berechtigte Anfrage erforderliche Informationen hierzu zur Verfügung.

§ 5 Unterauftragsverarbeiter und Drittlandtransfer

(1) Der Auftraggeber erteilt eine allgemeine Genehmigung für weitere Auftragsverarbeiter nach Art. 28 Abs. 2 DSGVO. Die derzeit vorgesehenen Dienstleister und Verarbeitungen sind in Anlage 3 beschrieben.

(2) Beabsichtigte Hinzuziehungen oder Ersetzungen teilt noplastics grundsätzlich mindestens 30 Tage vor Aufnahme der betreffenden Verarbeitung per E-Mail oder über eine dauerhaft abrufbare aktuelle Unterauftragsverarbeiterliste mit. Der Auftraggeber kann innerhalb von 14 Tagen aus sachlich begründeten datenschutzrechtlichen Gründen widersprechen. Ist keine zumutbare Lösung möglich, kann die betroffene Leistung außerordentlich beendet werden.

(3) Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter entsprechend Art. 28 Abs. 4 DSGVO zu im Wesentlichen gleichwertigen Schutzpflichten und bleibt dem Auftraggeber für deren Erfüllung verantwortlich.

(4) Übermittlungen in Drittländer finden ausschließlich nach Maßgabe der Art. 44 ff. DSGVO statt, insbesondere aufgrund eines anwendbaren Angemessenheitsbeschlusses oder geeigneter Standardvertragsklauseln einschließlich erforderlicher ergänzender Maßnahmen.

§ 6 Unterstützung und Datenschutzvorfälle

(1) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber durch angemessene Maßnahmen bei Betroffenenrechten nach Art. 12–22 DSGVO sowie – soweit erforderlich und auf Grundlage der ihm verfügbaren Informationen – bei Pflichten nach Art. 32–36 DSGVO.

(2) Anfragen betroffener Personen zu Auftragsdaten leitet noplastics unverzüglich an den Auftraggeber weiter. Eine inhaltliche Beantwortung erfolgt nur auf dessen Weisung oder aufgrund eigener rechtlicher Pflicht. Dies gilt auch für Shopify-Datenschutzwebhooks, soweit diese Auftragsdaten betreffen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Bekanntwerden über eine Verletzung des Schutzes personenbezogener Auftragsdaten. Die Mitteilung enthält die verfügbaren Informationen zu Art, Umfang, Folgen und ergriffenen Maßnahmen. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

(4) Der Auftragnehmer trifft angemessene Maßnahmen zur Eindämmung und Behebung eines Datenschutzvorfalls, dokumentiert ihn und unterstützt den Auftraggeber bei etwaigen Melde- und Benachrichtigungspflichten.

§ 7 Nachweise und Kontrollen

(1) noplastics stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung von Art. 28 DSGVO und dieses AVV erforderlich sind. Geeignete Sicherheitsdokumentationen, Prüfberichte und Zertifizierungen können vorrangig herangezogen werden.

(2) Soweit diese Informationen nicht ausreichen, ermöglicht noplastics erforderliche Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Vertraulichkeit verpflichteten Prüfer. Prüfungen erfolgen nach angemessener Ankündigung und mit Rücksicht auf Sicherheit, Geschäftsgeheimnisse

und Rechte anderer Kunden. Bei Vorfällen oder behördlichen Anforderungen sind erforderliche Sonderprüfungen möglich.

(3) Jede Partei trägt ihre eigenen Kosten. Soweit eine über gesetzlich erforderliche Nachweise hinausgehende Sonderprüfung außergewöhnlichen Zusatzaufwand verursacht, können die Parteien dessen angemessene Vergütung vorab vereinbaren. Zwingende Kontrollrechte bleiben unberührt.

§ 8 Rückgabe, Archivierung, Löschung

(1) Nach Ende der Auftragsverarbeitung löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Auftragsdaten oder gibt sie ihm zurück. Bestehende Kopien sind zu löschen, sofern nicht Unions- oder Mitgliedstaatenrecht eine Speicherung verlangt. Die vertraglich vorgesehene Exportfunktion kann zur Rückgabe genutzt werden.

(2) Der Auftraggeber erteilt seine Weisung über die angebotenen Export-, Lösch- und gegebenenfalls Archivierungsfunktionen oder in Textform. Soweit keine ausdrückliche Wahl getroffen wird und nach einer gesetzlich oder vertraglich vorgesehenen Export-/Übergangsphase keine weitere Auftragsverarbeitung zulässig ist, werden die Daten nach entsprechender vorheriger Information an den Auftraggeber gelöscht.

(3) Eine weitere Aufbewahrung personenbezogener Angaben innerhalb von technischen Dossiers oder Audit-Trails erfolgt nur im Rahmen einer zulässigen Beauftragung/Weisung des Auftraggebers. Der Auftraggeber bleibt für seine gesetzlichen Dokumentationsfristen verantwortlich.

(4) Sicherungskopien werden nach dem dokumentierten Backup-/Löschkonzept überschrieben oder gelöscht und bis dahin nur zur Sicherung bzw. Wiederherstellung vorgehalten. Eigene gesetzlich aufzubewahrende Vertrags- und Sicherheitsnachweise von noplastics bleiben – soweit zulässig – hiervon unberührt.

§ 9 Haftung

(1) Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Innenverhältnis gelten die gesetzlichen Verantwortungs- und Verursachungsregeln. Zwingende Ansprüche werden durch diesen AVV nicht beschränkt.

(2) Für Schäden aus Pflichten des Auftraggebers, insbesondere der Auswahl rechtswidriger Zwecke oder Daten, haftet noplastics nicht, soweit es den Schaden nicht durch eine eigene Pflichtverletzung verursacht oder mitverursacht hat. Im Übrigen gelten die Haftungsregeln des Hauptvertrags, soweit sie mit zwingendem Datenschutzrecht vereinbar sind.

§ 10 Laufzeit, Form und Schlussbestimmungen

(1) Dieser AVV wird bei Vertragsschluss in elektronischer Form mit dem Hauptvertrag vereinbart und gilt ab Beginn der ersten Auftragsverarbeitung für deren Dauer einschließlich einer gegebenenfalls vereinbarten nachvertraglichen Aufbewahrung. Eine isolierte Kündigung bei fortbestehender Auftragsverarbeitung ist ausgeschlossen.

(2) Änderungen erfolgen in Textform, soweit gesetzlich zulässig. Änderungen bei Unterauftragsverarbeitern und TOM unterliegen den besonderen Verfahren nach §§ 4 und 5.

(3) Es gilt deutsches Recht. Soweit gesetzlich zulässig ist Gerichtsstand der Sitz des Auftragnehmers. Bei Unwirksamkeit einzelner Regelungen gelten die gesetzlichen Vorschriften.

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb von noplastics-Webplattform und Shopify-App einschließlich Shopify-Import, Verpackungs-/Bestellzuordnung, technischer Dokumentation, OCR-/KI-Verarbeitung, Dossier-/DoC-Management, Freigaben, QR-/Prüfnachweisen, Audit-Trails, Lieferantenanfragen sowie Export-/Löschfunktionen.
Dauer	Dauer des Hauptvertrags einschließlich vereinbarter oder gesetzlich erforderlicher Export-/Übergangs-/Archivierungsphasen.

Merkmal	Beschreibung
Zwecke	Ausschließlich technische Bereitstellung der vom Händler beauftragten Funktionen, Nachweisführung, Dokumentenbeschaffung, Zuordnung und Verwaltung von Verpackungsdaten, Sendungen, Freigaben und Kontakten.
Verarbeitungsarten	Empfangen, Erheben, Auslesen, OCR/Extraktion, Speichern, Ordnen, Abgleichen, Zuordnen, Protokollieren, Übermitteln, Bereitstellen, Exportieren, Einschränken, Anonymisieren, Löschen.
Betroffene Personen	Beschäftigte und vertretungsberechtigte Nutzer des Händlers; Kunden des Händlers, soweit deren Daten in Shopify-Ereignissen/Dateien mitübertragen werden; Lieferanten-/Herstellerkontakte; natürliche Personen in technischen Dokumenten und Freigaben; ggf. Einzelunternehmer.
Datenkategorien	Shop-/Bestell-/Fulfillment-IDs, soweit personenbeziehbar; ggf. Namen, Liefer-/Kontakt-/Adressdaten und Bestellangaben; geschäftliche Kontakte; E-Mail- und Kommunikationsinhalte; Signaturen, Rollen, Nutzerkennungen, Zeit-/Freigabestempel; Angaben aus Hersteller-/Labor-/Compliance-Dokumenten; öffentliche Nachweisangaben nach Kundenfreigabe.
Besondere Kategorien	Besondere Kategorien i.S.d. Art. 9 DSGVO sind nicht vorgesehen. Der Auftraggeber soll sie nicht übermitteln; unbeabsichtigt eingehende Daten sollen frühzeitig gelöscht oder ausgeschlossen werden.
Shopify-Ereignisse	Empfang von shop- und bestellbezogenen Ereignissen, technischen Korrekturen sowie Datenschutzwebhooks; nur soweit erforderliche Daten anfordern und speichern.
OCR/KI	Automatische Analyse, Extraktion und Zuordnung technischer Datenblätter; externer Dienstleister nur nach den Anforderungen des AVV.
Supplier Requests	Auf Kundenweisung geschäftliche E-Mail-Kommunikation mit Lieferanten/Herstellern samt sachlicher Erinnerungen höchstens vier Wochen.
Öffentliche Seiten	Vom Auftraggeber veranlasste Freigabe und technische Bereitstellung von prüf- und sendungsbezogenen Statusseiten, ggf. Suche nach einer vom Händler bestimmten Kennung.
Datenflüsse/Empfänger	Unterauftragsverarbeiter gemäß Anlage 3; Veröffentlichung und Empfänger im Übrigen gemäß dokumentierter Kundeneinstellung und gesetzlicher Verpflichtung.

Anlage 2 – Technische und organisatorische Maßnahmen

noplastics gewährleistet ein dem jeweiligen Risiko angemessenes Schutzniveau. Die folgende Beschreibung legt Mindestschutzziele und Umsetzungsanforderungen fest. Konkrete technische Konfigurationen werden intern dokumentiert, regelmäßig überprüft und bei Bedarf aktualisiert.

Schutzziel	Mindestmaßnahme
Physische Sicherheit	Rechenzentrumssicherheit des eingesetzten Cloudanbieters; befugnisabhängiger Zugang zu eigener technischer Infrastruktur.
Authentifizierung	Individuelle, nachvollziehbare Zugänge; abgesicherte Anmeldeverfahren; angemessener Schutz administrativer Konten und Shopify-Autorisierungstoken.
Berechtigungen / Mandantentrennung	Rollen-/Rechtekontrollen nach Need-to-know; logische Trennung von Händlershops; Schutz vor unberechtigter Einsicht in fremde Daten, Bestellungen und Nachweise.
Transport / Schnittstellen	Verschlüsselte Übertragung (TLS/HTTPS), Integritätsprüfung von Shopify-Webhooks und sichere Aufbewahrung/Rotation von API-Zugangsdaten.

Schutzziel	Mindestmaßnahme
Datenspeicherung	Angemessene Cloud-Speicherabsicherung und Verschlüsselung ruhender Daten; möglichst EU-Regionen für primäre Datenhaltung; begrenzter Administratorenzugriff.
Protokollierung	Nachvollziehbarkeit sicherheitskritischer und kundenbezogener Freigabe-/Änderungsvorgänge; zweckmäßige, beschränkte Log-Speicherung und Schutz vor unbefugter Veränderung.
Öffentliche Prüfnachweise	Zugriffsschutz entsprechend Veröffentlichungsart, Schutz vor enumeration/erratenen Referenzen, Verhinderung ungewollter Offenlegung von Endkundendaten.
Datensparsamkeit	Beschränkung der Shopify-Scopes und Datenfelder auf benötigte Informationen; frühestmögliche Entfernung nicht benötigter personenbezogener Inhalte.
Verfügbarkeit / Backup	Angemessene Datensicherung, Wiederherstellbarkeit, Backup-Aufbewahrungs- und Löschkonzept; regelmäßige Wirksamkeitsprüfung.
Entwicklung / Incident	Sicherer Änderungsprozess, Patch- und Schwachstellenmanagement, Behandlung und Dokumentation von Sicherheits- und Datenschutzvorfällen.
Löschung / Dienstleister	Regelbasierte Löschung/Anonymisierung einschließlich Shopify-Datenschutzwebhooks und Backup-Zyklen; vertragliche Einbindung aller Unterauftragsverarbeiter und Kontrolle von Transfers.

Anlage 3 – Weitere Auftragsverarbeiter

Die nachstehende Liste bildet die bislang konkret benannten Dienstleister für personenbezogene Auftragsdaten ab.

Dienstleister	Aufgabe / Ort / Transfer
Google Cloud EMEA Limited bzw. die nach der tatsächlichen Cloud-Vertragsstruktur einschlägige Google-Gesellschaft	Hosting, Datenbank und Cloud-Infrastruktur; primäre Datenhaltung nach bisherigem Konzept in EU-Regionen. Etwaige weitere Zugriffe/Transfers nur nach Google Cloud DPA und Art. 44 ff. DSGVO.
Plus Five Five, Inc. (Resend), USA	Technischer Versand transaktionaler E-Mails und – soweit aktiv – Supplier Requests; Übermittlungen in die USA nur auf geeigneter Art.-44-ff.-Grundlage gemäß einschlägigem Anbieter-DPA.

Anlage 4 – Weisungskanäle und Vertragsschluss

Weisungen werden über autorisierte App-Funktionen (insbesondere Installation, Datenimporte, Dokumenten- und Rollenbestätigung, Freigabe, Veröffentlichung, Export, Löschung), über in Textform mitgeteilte Weisungen sowie über die im Hauptvertrag bestimmten Ansprechpartner erteilt. Datenschutzkontakt des Auftragnehmers: info@noplastics.de. Ansprechpartner des Auftraggebers ergibt sich aus dessen Händlerkonto bzw. der benannten geschäftlichen Kontaktadresse.

Dieser Vertrag wird wirksam durch elektronische Einbeziehung und Annahme im Buchungs-/Onboarding-Verfahren. Der konkrete Auftraggeber ergibt sich aus der Shopify-Shop-/Kundenidentifikation und den im Hauptvertrag angegebenen Unternehmensdaten. Eine gesonderte handschriftliche Unterzeichnung ist nicht erforderlich.