

VERTRAG ZUR AUFTRAGSVERARBEITUNG

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

für die B2B-SaaS-Plattform „noplastics“

Vertragsparteien

Dieser Vertrag zur Auftragsverarbeitung („AVV“) wird zwischen dem im Hauptvertrag als Kunde bezeichneten Unternehmer („Auftraggeber“ oder „Verantwortlicher“) und

noplastics UG (haftungsbeschränkt) i. G.

Mergelweg 5, 73760 Ostfildern, Deutschland

vertreten durch den Geschäftsführer Marc Trautwein

E-Mail: info@noplastics.de

– nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“ –

geschlossen. Der AVV ergänzt den Vertrag über die Nutzung der B2B-SaaS-Plattform noplastics einschließlich der jeweils gebuchten Funktionen („Hauptvertrag“). Er gilt für alle Verarbeitungsvorgänge, bei denen noplastics personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers verarbeitet.

§ 1 Gegenstand, Rollenverteilung und Rang

(1) Der Auftragnehmer verarbeitet die in Anlage 1 beschriebenen personenbezogenen Daten im Auftrag des Auftraggebers. Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die Kategorien betroffener Personen und personenbezogener Daten ergeben sich aus Anlage 1.

(2) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er ist insbesondere für die Rechtmäßigkeit der Verarbeitung, das Vorliegen einer geeigneten Rechtsgrundlage, die Erfüllung der Informationspflichten gegenüber betroffenen Personen sowie die Zulässigkeit und Richtigkeit seiner Weisungen verantwortlich.

(3) Soweit noplastics personenbezogene Daten für eigene Zwecke und in eigener datenschutzrechtlicher Verantwortlichkeit verarbeitet, insbesondere zur eigenen Vertragsverwaltung, Abrechnung, Forderungsbearbeitung, Missbrauchs- und IT-Sicherheitsprävention, Erfüllung eigener gesetzlicher Pflichten oder Verteidigung eigener Rechtsansprüche, findet dieser AVV auf diese Verarbeitung nicht Anwendung. Hierüber informiert noplastics gesondert in seiner Datenschutzerklärung.

(4) Soweit Regelungen dieses AVV und des Hauptvertrags dieselbe Auftragsverarbeitung betreffen und voneinander abweichen, geht dieser AVV vor. Im Übrigen bleibt der Hauptvertrag unberührt.

§ 2 Weisungsgebundene Verarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und nur in dem für die Erbringung der vereinbarten Leistungen erforderlichen Umfang. Dies gilt auch für Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation, soweit nicht eine unionsrechtliche oder mitgliedstaatliche Rechtsvorschrift den Auftragnehmer hierzu verpflichtet.

(2) Eine gesetzlich verpflichtende Verarbeitung außerhalb einer Weisung teilt der Auftragnehmer dem Auftraggeber vor Beginn der betreffenden Verarbeitung mit, sofern das anwendbare Recht eine solche Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

(3) Dokumentierte Weisungen ergeben sich insbesondere aus dem Hauptvertrag, diesem AVV, den innerhalb der Plattform durch autorisierte Nutzer vorgenommenen Uploads, Einstellungen, Freigaben, Supplier Requests, Export-, Archivierungs- oder Löschvorgängen sowie aus zusätzlichen Weisungen in Textform.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere anwendbare Datenschutzvorschriften verstößt. Er darf die Durchführung der betreffenden Weisung aussetzen, bis diese bestätigt, geändert oder rechtlich geklärt ist.

(5) Eine Nutzung personenbezogener Auftragsdaten für eigene Werbung, Adressvermarktung oder eigene Profilbildungszwecke des Auftragnehmers findet nicht statt.

§ 3 Plattformbezogene Verarbeitungen und Supplier Requests

(1) Der Auftragnehmer darf im Rahmen der vom Auftraggeber genutzten Plattformfunktionen personenbezogene Inhalte aus Shop-/Bestelldateien, Compliance- und Lieferantendokumenten, Audit-Trails, Freigabevorgängen und sonstigen vom Auftraggeber bereitgestellten Daten technisch entgegennehmen, strukturieren, zuordnen, speichern, extrahieren, abgleichen, bereitstellen und exportieren, soweit dies für den jeweiligen Workflow erforderlich ist.

(2) Soweit vollständige Shop- oder Bestelldateien, insbesondere CSV- oder XLSX-Dateien, personenbezogene Endkundendaten enthalten, verarbeitet noplastics diese ausschließlich im Auftrag des Auftraggebers. Nicht für den

vereinbarten Verpackungs-/Compliance-Workflow benötigte personenbezogene Daten werden nicht für eigene Zwecke genutzt und sind so früh wie technisch und betrieblich möglich aus dem operativen Verarbeitungsbestand zu entfernen oder von der weiteren Verarbeitung auszunehmen.

(3) Der Auftragnehmer darf technische Dokumente automatisiert auslesen und Inhalte mittels OCR oder vergleichbarer Extraktions- und Zuordnungsfunktionen verarbeiten. Die hierbei entstehenden personenbezogenen Angaben und Freigabe-/Prüfmetadaten bleiben Auftragsdaten des Auftraggebers. Soweit für solche Funktionen künftig ein weiterer externer Auftragsverarbeiter eingesetzt wird, richtet sich dessen Einbeziehung nach § 5.

(4) Der Auftraggeber weist den Auftragnehmer an und ermächtigt ihn, im Rahmen der Plattform im Namen und für Zwecke des Auftraggebers geschäftliche Lieferanten-, Hersteller-, Fulfillment- oder sonstige vom Auftraggeber bestimmte Ansprechpartner zu kontaktieren, soweit dies der Beschaffung fehlender produkt-, verpackungs- oder compliancebezogener Informationen und Nachweisdokumente dient.

(5) Die Supplier-Request-Weisung umfasst insbesondere die Verarbeitung von Namen, geschäftlichen E-Mail-Adressen, Funktionen und Unternehmenszugehörigkeiten, Kommunikationsinhalten, Versand- und Zustelldaten sowie empfangenen Antworten und Anhängen. Die Daten dürfen dem jeweiligen Produkt-, Verpackungs- oder Kundendatensatz zugeordnet und im Audit-Trail dokumentiert werden.

(6) Aktiviert der Auftraggeber die automatisierte Supplier-Request-Funktion oder löst er einen Supplier Request aus, darf der Auftragnehmer eine Erstanfrage sowie die im System vorgesehenen sachlichen Erinnerungs- und Nachfassnachrichten innerhalb eines Zeitraums von höchstens vier Wochen versenden. Nach Ablauf dieses Zeitraums erfolgt ohne erneute Weisung des Auftraggebers keine weitere automatisierte Kontaktaufnahme.

(7) Die Supplier-Request-Kommunikation dient ausschließlich der Beschaffung und Dokumentation der bezeichneten Unterlagen bzw. Informationen. Eigene Werbung des Auftragnehmers gegenüber den kontaktierten Personen ist hiervon nicht umfasst.

(8) Der Auftraggeber bleibt dafür verantwortlich, dass die von ihm bestimmten Lieferantenkontakte rechtmäßig verwendet werden dürfen und erforderliche Informationspflichten gegenüber den betroffenen Personen erfüllt werden. Der Auftragnehmer kann auf Weisung einen vom Auftraggeber freigegebenen Datenschutzhinweis oder Link technisch in die Kommunikation einbinden.

(9) Soweit der Auftraggeber öffentliche oder zugangsbeschränkte QR-/Statusseiten aktiviert, darf noplastics die hierfür vom Auftraggeber freigegebenen personenbezogenen Inhalte technisch bereitstellen. Über Inhalt, Umfang und Freigabe entscheidet der Auftraggeber.

§ 4 Vertraulichkeit und Sicherheit der Verarbeitung

(1) Der Auftragnehmer stellt sicher, dass sich alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die Daten nur im Rahmen ihrer Befugnisse verarbeiten.

(2) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

(3) Die bei Vertragsschluss geltenden Mindestmaßnahmen sind in Anlage 2 beschrieben. Der Auftragnehmer darf technische und organisatorische Maßnahmen weiterentwickeln oder durch gleichwertige bzw. wirksamere Maßnahmen ersetzen, sofern das Schutzniveau insgesamt nicht abgesenkt wird.

(4) Der Auftragnehmer überprüft die Wirksamkeit seiner Schutzmaßnahmen in angemessenen Abständen und passt sie bei wesentlichen technischen, organisatorischen oder risikobezogenen Änderungen an.

§ 5 Weitere Auftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten weiteren Auftragsverarbeiter sind in Anlage 3 aufgeführt.

(2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter grundsätzlich mindestens 30 Tage vor Beginn der betreffenden Verarbeitung. Die Information kann per E-Mail oder über eine dauerhaft abrufbare aktuelle Unterauftragsverarbeiterliste erfolgen.

(3) Der Auftraggeber kann einer Änderung innerhalb von 14 Tagen nach Zugang der Information aus sachlich begründeten datenschutzrechtlichen Gründen widersprechen. Die Parteien werden zunächst versuchen, eine zumutbare Lösung zu finden. Ist der Einsatz des betreffenden Dienstleisters für die betroffene Leistung technisch erforderlich und lässt sich keine zumutbare Alternative herstellen, kann jede Partei den hiervon betroffenen Leistungsbestandteil außerordentlich beenden.

(4) Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter vertraglich zu Datenschutzpflichten, die im Wesentlichen denselben Schutzstandard wie dieser AVV gewährleisten und den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen.

Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

(5) Soweit eine Verarbeitung außerhalb des Europäischen Wirtschaftsraums stattfindet, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies kann insbesondere durch einen Angemessenheitsbeschluss, die EU-US Data Privacy Framework-Zertifizierung eines Empfängers oder Standardvertragsklauseln der Europäischen Kommission einschließlich gegebenenfalls erforderlicher ergänzender Schutzmaßnahmen erfolgen.

§ 6 Betroffenenrechte

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und soweit möglich durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers aus Art. 12 bis 22 DSGVO.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer wegen einer diesem AVV unterliegenden Verarbeitung, leitet der Auftragnehmer das Ersuchen ohne unangemessene Verzögerung an den Auftraggeber weiter. Eine inhaltliche Beantwortung erfolgt nur auf Weisung des Auftraggebers oder aufgrund einer eigenen gesetzlichen Verpflichtung.

(3) Zur Umsetzung zulässiger Weisungen darf der Auftragnehmer insbesondere Such-, Export-, Berichtigungs-, Einschränkungs-, Sperr- und Löschvorgänge durchführen.

§ 7 Unterstützungs-, Nachweis- und Meldepflichten

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen angemessen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

(2) Der Auftragnehmer informiert den Auftraggeber über eine Verletzung des Schutzes personenbezogener Daten, die von diesem AVV erfasste Auftragsdaten betrifft, unverzüglich nach Bekanntwerden.

(3) Die Mitteilung enthält, soweit verfügbar, die Informationen, die der Auftraggeber zur Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO benötigt, insbesondere Art des Vorfalls, betroffene Daten- und Personenkategorien, voraussichtliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen. Informationen dürfen schrittweise nachgereicht werden, soweit sie noch nicht vollständig vorliegen.

(4) Der Auftragnehmer trifft unverzüglich angemessene Maßnahmen zur Eindämmung und Behebung des Vorfalls sowie zur Minderung möglicher nachteiliger Folgen und dokumentiert Datenschutzverletzungen nach den gesetzlichen Anforderungen.

(5) Der Auftragnehmer führt, soweit gesetzlich erforderlich, ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt der zuständigen Aufsichtsbehörde dieses auf Anfrage zur Verfügung. Einen Datenschutzbeauftragten bestellt der Auftragnehmer, soweit die gesetzlichen Voraussetzungen hierfür vorliegen.

§ 8 Informationen und Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber die Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO und diesem AVV nachzuweisen.

(2) Der Nachweis soll vorrangig durch geeignete Dokumentationen, Sicherheitsinformationen, vorhandene Prüfberichte, Zertifizierungen oder sonstige geeignete Nachweise erfolgen.

(3) Soweit solche Nachweise für eine erforderliche Kontrolle nicht ausreichen, darf der Auftraggeber selbst oder durch einen zur Vertraulichkeit verpflichteten sachkundigen Prüfer nach angemessener Vorankündigung während der üblichen Geschäftszeiten eine weitergehende Prüfung durchführen. Prüfungen sind auf den erforderlichen Umfang zu beschränken und so zu organisieren, dass Geschäftsgeheimnisse, IT-Sicherheit, der Geschäftsbetrieb und Rechte anderer Kunden nicht unverhältnismäßig beeinträchtigt werden.

(4) Ohne konkreten Anlass sollen Vor-Ort-Prüfungen grundsätzlich nicht häufiger als einmal innerhalb von zwölf Monaten verlangt werden. Diese Beschränkung gilt nicht bei erheblichen Datenschutzvorfällen, begründeten Anhaltspunkten für einen wesentlichen Verstoß oder einer Anordnung der zuständigen Aufsichtsbehörde.

(5) Jede Partei trägt ihre eigenen Prüfungskosten. Verursacht eine vom Auftraggeber veranlasste Prüfung beim Auftragnehmer einen erheblichen Zusatzaufwand, der über die gesetzlichen Nachweis- und Mitwirkungspflichten hinausgeht, kann dieser nach vorheriger Abstimmung angemessen berechnet werden, es sei denn, die Prüfung weist einen wesentlichen vom Auftragnehmer zu vertretenden Datenschutzverstoß nach.

§ 9 Rückgabe, Export, Archivierung und Löschung

(1) Die Auftragsverarbeitung besteht für die Dauer des Hauptvertrags und, soweit vom Auftraggeber beauftragt, während einer nachvertraglichen Export-, Übergangs- oder Archivierungsphase fort.

(2) Nach Beendigung der Auftragsverarbeitung löscht oder gibt der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Auftragsdaten zurück, soweit nicht eine unionsrechtliche oder mitgliedstaatliche Rechtsvorschrift die weitere Speicherung verlangt. Die vertraglich vorgesehene Exportfunktion gilt als Möglichkeit der Rückgabe. Der

Auftraggeber hat die gewünschte Rückgabe bzw. einen Export innerhalb der im Hauptvertrag vorgesehenen Abruf- oder Übergangsfrist zu veranlassen.

(3) Soweit personenbezogene Angaben Bestandteil von Compliance-Dokumenten, Audit-Trails oder Nachweisakten sind, kann der Auftraggeber noplastics anweisen, diese im Rahmen der vereinbarten Archivierungsfunktion für die vom Auftraggeber benötigte Dauer weiter im Auftrag vorzuhalten. Die datenschutzrechtliche Zulässigkeit und Dauer dieser Archivierungsweisung verantwortet der Auftraggeber.

(4) Nach Ablauf der vereinbarten Rückgabe-, Abruf- oder Archivierungsfrist löscht oder anonymisiert der Auftragnehmer die Auftragsdaten, soweit keine zulässige abweichende Weisung oder gesetzliche Speicherpflicht besteht.

(5) Gesetzlich erforderliche oder zur Verteidigung eigener Rechtsansprüche notwendige Nachweise über die ordnungsgemäße Leistungserbringung und Auftragsverarbeitung darf der Auftragnehmer in eigener Verantwortlichkeit für die hierfür erforderliche Dauer aufbewahren.

(6) Daten in Sicherungskopien werden im Rahmen der regulären Backup- und Löschzyklen überschrieben oder gelöscht und bis dahin ausschließlich für Wiederherstellungs- und Sicherheitszwecke vorgehalten.

§ 10 Haftung

(1) Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Innenverhältnis tragen die Parteien Schäden, erforderliche Aufwendungen und behördliche Sanktionen entsprechend ihrem jeweiligen Verantwortungs- und Verursachungsanteil sowie nach Maßgabe der sonstigen vertraglichen und gesetzlichen Haftungsregelungen.

(2) Der Auftragnehmer ist nicht für die Rechtmäßigkeit der vom Auftraggeber bestimmten Zwecke, die Auswahl der betroffenen Personen, die rechtliche Zulässigkeit der vom Auftraggeber bereitgestellten Kontakt- oder Inhaltsdaten oder die materielle Richtigkeit der vom Auftraggeber bzw. dessen Lieferanten übermittelten Inhalte verantwortlich, soweit der Auftragnehmer nicht selbst über Zwecke und wesentliche Mittel entscheidet oder ausdrücklich eine eigene Prüfpflicht übernommen hat.

(3) Im Übrigen gelten die Haftungsregelungen des Hauptvertrags, soweit sie mit zwingenden datenschutzrechtlichen Vorschriften vereinbar sind.

§ 11 Laufzeit, Vertragsschluss und Schlussbestimmungen

(1) Dieser AVV tritt spätestens mit Beginn der ersten Auftragsverarbeitung in Kraft und gilt für deren Dauer. Solange der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, kann der AVV nicht isoliert beendet werden.

(2) Der AVV kann als Bestandteil des elektronischen Buchungs- bzw. Registrierungsprozesses geschlossen und in elektronischer Form gespeichert werden. Eine gesonderte handschriftliche Unterzeichnung ist nicht erforderlich.

(3) Änderungen und Ergänzungen dieses AVV einschließlich seiner Anlagen können in Textform erfolgen, soweit keine strengere Form gesetzlich vorgeschrieben ist. Änderungen der Unterauftragsverarbeiter richten sich ausschließlich nach § 5. Technische Weiterentwicklungen der TOM nach § 4 bedürfen keiner individuellen Neuvereinbarung, sofern das Schutzniveau nicht abgesenkt wird.

(4) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig und beide Parteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen sind, der Sitz des Auftragnehmers.

(5) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Regelung treten die gesetzlichen Vorschriften.

Anlage 1 – Beschreibung der Auftragsverarbeitung

Merkmal	Beschreibung
Gegenstand	Bereitstellung und Betrieb der B2B-SaaS-Plattform noplastics einschließlich Daten-/Dateiimport, Verpackungs- und Auftragszuordnung, automatisierter Dokumentenauslesung/OCR, Compliance-Dokumentenmanagement, Supplier Requests, Audit-Trail, Freigabe-/Signatur-Workflows, QR-/Statusfunktionen, Export und kundenbezogener Archivierung.
Dauer	Für die Dauer des Hauptvertrags sowie etwaiger vom Auftraggeber beauftragter Export-, Übergangs- oder Archivierungszeiträume.
Zwecke	Technische Erbringung der vom Auftraggeber gebuchten Plattformleistungen; Extraktion und Zuordnung von Daten; Verwaltung und Dokumentation von Verpackungs-/Compliance-Prozessen; Beschaffung fehlender Lieferanteninformationen und Nachweise; Dokumentation von Freigaben und Prozessschritten; Bereitstellung kundenbezogener Ausgaben, Dokumente, QR-/Statusseiten und Exporte.
Art der Verarbeitung	Erheben/Entgegennehmen, Übermitteln, Erfassen, Auslesen/OCR, Extrahieren, Ordnen, Strukturieren, Speichern, Abgleichen, Filtern, Zuordnen, Plausibilisieren, Protokollieren, Bereitstellen, Exportieren, Einschränken, Archivieren, Löschen und Anonymisieren.
Betroffene Personen	Beschäftigte, Geschäftsführer und sonstige autorisierte Nutzer/Ansprechpartner des Auftraggebers; Endkunden des Auftraggebers, soweit deren Daten in Shop-/Bestellimporten technisch enthalten sind; Ansprechpartner bei Lieferanten, Herstellern, Fulfillment-/Logistikunternehmen und Laboren; Unterzeichner und sonstige natürliche Personen in technischen, Labor-, Prüf-, Hersteller- oder Lieferantendokumenten; gegebenenfalls Einzelunternehmer und sonstige natürliche Geschäftspartner.
Datenkategorien	Name, geschäftliche Kontakt- und Funktionsdaten, Unternehmenszugehörigkeit; Kommunikationsinhalte und E-Mail-Metadaten; personenbezogene Inhalte und Unterschriften in Dokumenten; Bestell-/Auftragsnummern; soweit technisch mitübertragen: Endkundenstamm-, Adress-, Kontakt- und Bestelldaten; kundenbezogene Audit-, Freigabe- und Signaturmetadaten; IP- und technische Identifikationsdaten, soweit sie im auftragsbezogenen Workflow anfallen.
Besondere Kategorien nach Art. 9 DSGVO	Nicht vorgesehen. Der Auftraggeber soll keine besonderen Kategorien personenbezogener Daten in die Plattform einstellen. Werden solche Daten unbeabsichtigt mitübertragen, dürfen sie nicht zweckfremd genutzt werden und sind, soweit möglich, frühzeitig zu entfernen bzw. zu löschen.
Shop-/Dateiimport	noplastics darf hochgeladene Shop-/Bestell- und Produktdaten technisch entgegennehmen und verarbeiten, um die für Verpackungs-, Auftrags- und Compliance-Workflows benötigten Informationen zu extrahieren. Nicht benötigte personenbezogene Endkundendaten werden nicht für eigene Zwecke verwendet und sind so früh wie technisch und betrieblich möglich aus der weiteren operativen Verarbeitung

	auszunehmen.
OCR / Dokumentenextraktion	noplastics darf technische Unterlagen automatisiert auslesen, strukturieren und dem betreffenden Datensatz zuordnen. Die Verarbeitung umfasst auch in Dokumenten enthaltene Namen, Kontaktdaten, Funktionen, Unterschriften und sonstige personenbezogene Angaben sowie die daraus erzeugten Extraktions- und Zuordnungsmetadaten.
Supplier Requests	Auf Weisung des Auftraggebers Versand einer Erstanfrage und sachlicher Nachfassnachrichten an vom Auftraggeber bestimmte Lieferanten-/Herstellerkontakte, Entgegennahme von Antworten und Anhängen und Zuordnung zum Kundendatensatz. Ohne erneute Weisung endet die automatisierte Kontaktphase spätestens nach vier Wochen.
Audit-/Freigabeprozess	Protokollierung kundenbezogener Uploads, Änderungen, Supplier Requests, Statusänderungen, Prüfungen, Freigaben und elektronischer Bestätigungen, soweit dies der Nachvollziehbarkeit des vom Auftraggeber gesteuerten Workflows dient.
QR-/Statusseiten	Soweit vom Auftraggeber aktiviert, technische Bereitstellung der von ihm freigegebenen Inhalte auf öffentlichen oder zugangsbeschränkten QR-/Statusseiten. Der Auftraggeber entscheidet über Inhalt und Freigabe.
Informationspflichten	Der Auftraggeber bleibt für die Erfüllung seiner Informationspflichten nach Art. 13 und 14 DSGVO verantwortlich. noplastics kann auf Weisung einen vom Auftraggeber freigegebenen Hinweis oder Link technisch in Supplier-Request-Kommunikation bzw. andere Workflows einbinden.

Anlage 2 – Technische und organisatorische Maßnahmen

noplastics verpflichtet sich, mindestens die nachfolgenden, dem jeweiligen Risiko angemessenen technischen und organisatorischen Maßnahmen aufrechtzuerhalten. Gleichwertige oder wirksamere Maßnahmen können an ihre Stelle treten.

Maßnahmenbereich	Umsetzung
Zutrittskontrolle	Betrieb der produktiven Infrastruktur über professionelle Cloud-Rechenzentren; physische Zutrittskontrollen und Rechenzentrumssicherheit werden durch den eingesetzten Cloudanbieter gewährleistet.
Zugangskontrolle	Personenbezogene bzw. eindeutig zuordenbare Nutzerkonten; authentifizierter Plattformzugang; nach aktuellem Produktkonzept passwortloser Login über einen an die registrierte E-Mail-Adresse versandten Anmeldelink; administrative Zugänge ausschließlich für berechtigte Personen.
Zugriffskontrolle	Rollen- und berechtigungsbezogene Zugriffsbeschränkung nach dem Need-to-know-Prinzip; Beschränkung administrativer Zugriffe; regelmäßige Überprüfung von Berechtigungen; Vertraulichkeitsverpflichtung berechtigter Personen.
Mandantentrennung	Logische Trennung kundenbezogener Daten innerhalb der SaaS-Anwendung und Datenhaltung; Schutz vor unberechtigtem Zugriff anderer Kunden.
Übertragungssicherheit	Verschlüsselte Übertragung der Plattformkommunikation über TLS/HTTPS; kontrollierte API-/Schnittstellenzugriffe; Nutzung hierfür vorgesehener Kommunikationsdienste für Supplier Requests.

Speicherung/Verschlüsselung	Primäre Datenhaltung in konfigurierten europäischen Google-Cloud-Regionen. Bei Google Cloud gespeicherte Kundeneinhalte werden standardmäßig im Ruhezustand verschlüsselt; Zugriffe erfolgen über berechtigungsgesteuerte Dienste und Konten.
Protokollierung/Nachvollziehbarkeit	Technische Protokollierung sicherheits- und funktionsrelevanter Ereignisse sowie kundenbezogener Audit-Trail für die vorgesehenen Compliance- und Freigabeprozesse. Protokolle werden zweckgebunden und nur für angemessene Zeiträume aufbewahrt.
Verfügbarkeit/Wiederherstellung	Angemessene, dem Risiko entsprechende Sicherungs- und Wiederherstellungsmaßnahmen für persistent gespeicherte produktive Daten; Nutzung der Redundanz- und Wiederherstellungsfunktionen der eingesetzten Cloud-Infrastruktur; Überprüfung der Wiederherstellbarkeit in angemessenen Abständen.
Integrität/Änderungsmanagement	Kontrollierte Softwareänderungen und Bereitstellungen; Begrenzung produktiver Änderungen auf berechtigte Personen; Sicherheits- und Fehlerbehebung; nachvollziehbare Behandlung wesentlicher Änderungen.
Incident Response	Organisatorisches Verfahren zur Erkennung, Bewertung, Eindämmung, Behebung und Dokumentation von Sicherheits- und Datenschutzvorfällen sowie zur unverzüglichen Eskalation an zuständige Personen.
Löschung	Kontrollierte Lösch- und Anonymisierungsprozesse nach Ablauf von Vertrags-, Export- und Archivierungsfristen; Berücksichtigung regulärer Backup-Zyklen.
Unterauftragnehmermanagement	Datenschutzrechtliche und vertragliche Einbindung weiterer Auftragsverarbeiter, Pflege einer aktuellen Unterauftragsverarbeiterübersicht und Prüfung erforderlicher Drittlandtransfermechanismen.

Anlage 3 – Genehmigte weitere Auftragsverarbeiter

Dienstleister	Leistung	Verarbeitungsort	Datenschutz-/Transfermechanismus
Google Cloud EMEA Limited	Cloud-Hosting, Cloud Run, Rechen-/Infrastruktur- und Datenhaltungsleistungen	Primäre Verarbeitung der Nutzdaten in konfigurierten EU-Regionen; weitere Verarbeitung nach Google Cloud DPA	Art. 28 DSGVO; für etwaige Drittlandübermittlungen die nach dem Google Cloud DPA vorgesehenen Mechanismen, insbesondere Angemessenheitsbeschlüsse bzw. Standardvertragsklauseln
Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA	Transaktionaler E-Mail-Versand, insbesondere Systemnachrichten und Supplier Requests, Zustell- und Kommunikationsmetadaten	USA; weitere Unterauftragsverarbeiter nach der jeweils aktuellen Resend-Unterauftragsverarbeiterliste	Art. 28 DSGVO; für Drittlandübermittlungen die im Resend-DPA vorgesehenen geeigneten Garantien, insbesondere Standardvertragsklauseln, soweit erforderlich

Anlage 4 – Weisungs- und Kommunikationskanäle

Weisungen können durch vertretungsberechtigte Personen des Auftraggebers sowie durch von ihm innerhalb der Plattform autorisierte Nutzer im Rahmen ihrer Berechtigungen erteilt werden. Technische Weisungen ergeben sich insbesondere aus Uploads, Freigaben, Aktivierung von Supplier Requests, QR-/Statusfreigaben, Export-, Archivierungs- und Löschfunktionen sowie sonstigen kundenbezogenen Einstellungen.

Zusätzliche Weisungen sowie datenschutzbezogene Mitteilungen des Auftraggebers können an die von noplastics bereitgestellte Support-/Kontaktadresse gerichtet werden. Datenschutzkontakt des Auftragnehmers: info@noplastics.de.

Vertragsschluss

Der Auftraggeber schließt diesen AVV durch Einbeziehung in den elektronischen Buchungs- oder Registrierungsprozess bzw. durch sonstige Vereinbarung in Textform. Die Bezeichnung und Kontaktdaten des Auftraggebers ergeben sich aus dem Hauptvertrag bzw. dem zugehörigen Kundenkonto. Der AVV ist dort in speicherbarer Form bereitzustellen.