

VEREINBARUNG

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

>>FIRMENNAME<<
>>STRAÙE<<
>>PLZ und ORT<<
>>LAND<<

>>Kunden-Nr<<

(im Folgenden „Verantwortlicher“)

Der Auftragsverarbeiter:

Austria Bio Garantie GmbH
oder
agroVet GmbH
Königsbrunnerstraße 8
2202 Enzersfeld

(im Folgenden „Auftragsverarbeiter“)

1. GEGENSTAND DER VEREINBARUNG

Diese Vereinbarung ergänzt alle zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgeschlossenen Vereinbarungen (Kontrollvereinbarungen, Zertifizierungsvereinbarungen).

Die in den genannten Vereinbarungen enthaltenen datenschutzrechtlichen Bestimmungen inklusive der bestehenden datenschutzrechtlichen Dienstleistungsvereinbarungen werden durch diese Vereinbarung neu geregelt.

Der Verantwortliche und der Auftragsverarbeiter verpflichten sich im Rahmen der Vertragsbeziehung bei der Verarbeitung personenbezogener Daten das österreichische Datenschutzgesetz (DSG) und die Datenschutz-Grundverordnung (DSGVO) sowie sonstige datenschutzrechtliche Bestimmungen in der jeweils geltenden Fassung ausnahmslos einzuhalten und alle erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit zu treffen.

Personenbezogene Daten, von welchen die Parteien im Zuge der Vertragsbeziehung Kenntnis erlangen, werden die Vertragsparteien ausschließlich zur Durchführung dieser Vertragsbeziehung verarbeiten. Eine darüber hinausgehende Datenverarbeitung ist nicht gestattet, sofern keine anderslautende schriftliche Weisung durch den jeweils anderen erfolgt. Der Auftragsverarbeiter ist gemäß ISO 17065 akkreditiertes Unternehmen und somit zur Einhaltung der Normvorgaben und insbesondere zur Verschwiegenheit verpflichtet.

Folgende Datenkategorien werden zur Erreichung des Vereinbarungszwecks verarbeitet: Stammdaten von Vertragspartnern (z.B. Name, Adresse, Kontaktdaten), Betriebsdaten, Vertragsdaten sowie Korrespondenz.

2. DAUER DER VEREINBARUNG

Die Ergänzung wird für die in der jeweiligen Vereinbarung erforderliche Dauer der Abwicklung abgeschlossen.

3. PFLICHTEN DES AUFTRAGSVERARBEITERS

- 3.1. Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Verantwortlichen zu verarbeiten. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so wird er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber informieren und die Behörde an diesen verweisen.

Paraphen

--	--

- 3.2. Der Auftragsverarbeiter erklärt, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.
- 3.3. Der Auftragsverarbeiter erklärt, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen).
- 3.4. Der Auftragsverarbeiter ergreift die technischen und organisatorischen Maßnahmen, damit der Verantwortliche die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und erkennt dieser, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, wird der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterleiten und dies dem Antragsteller mitteilen.
- 3.5. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation). Für den mit den Leistungen nach Punkt 3.8. zusammenhängenden Aufwand kann der Auftragsverarbeiter dem Verantwortlichen ein Entgelt nach Maßgabe der dem zu Punkt 1 beschriebenen Vertrag zugrundeliegenden Tarife verrechnen.
- 3.6. Der Auftragsverarbeiter hat für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO errichtet.
- 3.7. Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Im Zweifelsfall kann der Auftragnehmer zusätzliche Information zur Bestätigung der Identität einfordern. Sollte der Verantwortliche offenkundig unbegründet und besonders häufig sein Recht auf Auskunft wahrnehmen, kann ein angemessenes Bearbeitungsentgelt verlangt werden bzw. die Bearbeitung des Antrages verweigert werden.
- 3.8. Im Falle der Beendigung der Vereinbarung gemäß Punkt 1 müssen die Aufbewahrungspflichten sowie die Vorgaben der Akkreditierung der Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, berücksichtigt werden (Löschung, Anonymisierung, etc.).
- 3.9. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, falls er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen Datenschutzbestimmungen der Union oder der Mitgliedsstaaten verstößt.

4. PFLICHTEN DES VERANTWORTLICHEN

- 4.1. Der Verantwortliche wird den Auftragsverarbeiter im Rahmen des Zumutbaren unterstützen, die Einhaltung der Bestimmungen der DSGVO sowie anwendbarer nationaler Datenschutzgesetze nachzuweisen und dem Auftragsverarbeiter auf Anfrage die hierfür erforderlichen Informationen zur Verfügung stellen.

Paraphen

--	--

- 4.2. Er ist verpflichtet, für die vorliegende Auftragsverarbeitung gemäß der in seinem alleinigen Verantwortungsbereich liegenden gesetzlichen Verpflichtung als Verantwortlicher der Datenverarbeitung ein Verarbeitungsverzeichnis nach Art 30 Absatz 1 DSGVO zu errichten.
- 4.3. Der Verantwortliche wird weiters während der aufrechten Vereinbarung den Auftragsverarbeiter vor einer Änderung der oben genannten Informationen rechtzeitig Bescheid geben, um das Verarbeitungsverzeichnis des Auftragsverarbeiters anzupassen.
- 4.4. Der Verantwortliche ist verpflichtet, den Auftragsverarbeiter bei den zu setzenden Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO bestmöglich zu unterstützen und empfohlene Maßnahmen umsetzen. Der Verantwortliche anerkennt, dass der Auftragsverarbeiter nicht die Sicherheit der Verarbeitung gewährleisten kann, soweit diese nicht mehr im alleinigen Verantwortungs- und Einflussbereich des Auftragsverarbeiters liegt oder der Verantwortliche vom Auftragsverarbeiter empfohlene Datensicherheitsmaßnahmen nicht umsetzt oder berücksichtigt.

5. HAFTUNG

- 5.1. Die zwischen den Parteien in der in Pkt. 1 genannte/n Vereinbarung/en vereinbarte Haftungsregelung gilt zwischen den Parteien auch für die Auftragsverarbeitung, sofern nichts anderes schriftlich vereinbart wird.

6. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

7. SUB-AUFTRAGSVERARBEITER

- 7.1. Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter hinzuziehen. Er hat den Verantwortlichen von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters rechtzeitig zu verständigen.
- 7.2. Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingetht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen.

8. ALLGEMEINE BESTIMMUNGEN

Ergänzend gelten sämtliche Bestimmungen der in Pkt. 1 getroffenen Vereinbarungen auch für diese Vereinbarung.

.....
[Ort], am [Datum]

.....
[Ort], am [Datum]

Für den Verantwortlichen:

Für den Auftragsverarbeiter:

.....
Rechtsgültige Zeichnung

.....
Rechtsgültige Zeichnung

Paraphen

--	--

Anlage 1

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Chipkarten-/Transponder-Schließsystem

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Zuordnung von Benutzerrechten

Erstellen von Benutzerprofilen

Passwortvergabe

Einsatz von VPN-Technologie

Authentifikation mit Benutzername / Passwort

Zuordnung von Benutzerprofilen zu IT-Systemen

Einsatz von Intrusion-Detection-Systemen

Einsatz einer Software-Firewall

Einsatz von Anti-Viren-Software

Einsatz einer Hardware-Firewall

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogener Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Passworrichtlinie inkl. Passwortlänge, Passwortwechsel

ordnungsgemäße Vernichtung von Datenträgern (DIN 32757 oder ÖNORM S 2109-1)

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Einrichtungen von Standleitungen bzw. VPN-Tunneln

Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen

Beim physischen Transport: sichere Transportbehälter/-verpackungen

Paraphen

--	--

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Teilweise Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Teilweise Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Erstellen eines Backup & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

Paraphen

--	--