AGREEMENT

on

data processing according to Art. 28 GDPR

The controller:

>>Company Name<<
>>Address<<

Customer number: «Nummer1»

(hereinafter referred to as "controller")

The processor:

Austria Bio Garantie GmbH
Königsbrunnerstrasse 8
2202 Enzersfeld

(hereinafter referred to as “processor”)

1. SUBJECT OF AGREEMENT

This agreement supplements all agreements concluded between the controller and the processor (inspection agreements, certification agreements).

The data protection regulations contained in the afore mentioned agreements, including the existing data protection service agreements, will be revised by this agreement.

In the course of the contractual relationship the controller and the processor undertake to comply with the national Data Protection Act (DPA) and the European General Data Protection Regulation (GDPR) as well as other data protection regulations as amended and to take all necessary technical and organizational measures for data security during the processing of personal data.

Personal data, which is acquired by the parties in the course of the contractual relationship, may only be processed by the contracting parties for the execution of this contractual relationship. Any further data processing is not permitted, unless otherwise agreed to in writing by the other contracting party.
The processor is an accredited company according to ISO 17065 and thus obliged to comply with the standards and in particular confidentiality.

The following categories of data are processed to achieve the purpose of the agreement: Master data of contract partners (e.g. name, address, contact details), company data, contract data and correspondence.

2. DURATION OF AGREEMENT

The supplement is completed for the required duration of the processing in the respective agreement.

3. OBLIGATIONS OF THE PROCESSOR

3.1. The processor undertakes to process data and processing results only in the context of the written instructions of the controller. If the processor receives an official order by an authority to provide data of controller, he will - if legally permissible - inform the controller without delay and refer the authority to the latter.

Initials

3.2. The processor declares that he has obligated all persons entrusted with data processing to confidentiality prior to commencing the activity or that they are subject to an appropriate obligation to secrecy. In particular, the confidentiality obligation of the persons responsible for data processing remains valid even after the termination of their duties and their departure from the processor.

3.3. The processor declares that he has taken all necessary measures to ensure the safety of processing under Article 32 GDPR (see Annex 1 for details).

3.4. The processor shall take the technical and organizational measures to enable the controller to comply at all times with the rights of the data subject under Chapter III of the GDPR (information, disclosure, correction and deletion, data portability, disagreement and automated decision-making in individual cases) within the statutory time limits and leaves the controller all necessary information. If a request is made to the processor and the processor realizes that the claimant mistakenly considers him responsible for the data application he is operating, the processor will immediately forward the request to the controller and notify the claimant.

3.5. The processor shall assist the controller in complying with the obligations set out in Articles 32 to 36 of the GDPR (data security measures, personal data breach notifications to the supervisory authority, notification of people affected by a data breach, data protection impact assessment, prior consultation). For the expenses associated with the services referred to in point 3.8, the processor may charge the controller in accordance with the tariffs on which the contract described in point 1 is based.

3.6. The processor has set up a processing directory in accordance with Art. 30 GDPR for this data processing.

3.7. The controller or a third party instructed by him is granted the right of access and control to the processing of the data provided by him at any time by the data processing facilities. The processor undertakes to provide the controller with the information that is necessary to control compliance with the obligations named in this agreement. In case of doubt, the contractor may request additional information to confirm the identity. Should the controller exercise his right to information manifestly unfounded and particularly often, a reasonable processing fee may be demanded or the request may be refused.

3.8. In case of termination of the agreement under point 1, the retention obligations and the specifications of the accreditation of the processing results and documents containing data must be taken into account (deletion, anonymization, etc.).

3.9. The processor will notify the controller without delay if he believes that the controller’s instructions violate the data protection provisions of the Union or the member states.

4. OBLIGATIONS OF THE CONTROLLER

4.1. The controller will support the processor as far as reasonably practicable to prove compliance with the provisions of the GDPR and applicable national data protection laws and provide the processor with the necessary information upon request.

Initials | | |

4.2. He is obliged to set up a processing directory according to Art. 30 (1) DSGVO for the current order processing in accordance with the legal obligation in his role as controller.

4.3. The controller will also, in due course during the upstanding agreement, notify the processor in advance of any change in the above information in order to adjust the processor's processing directory.

4.4. The controller is obliged to provide the best possible support to the processor in the measures to be taken to ensure the safety of the processing according to Art. 32 GDPR and to implement recommended measures. The controller acknowledges that the processor can not guarantee the safety of the processing, if it is no longer the sole responsibility and sphere of influence of the processor or the controller does not implement or take into account data protection measures recommended by the processor.

5. LIABILITY

5.1. The liability clause agreed between the parties in the agreement referred to in point 1 shall also apply between the parties to the data processing, unless otherwise agreed in writing.

6. PLACE OF EXECUTION OF DATA PROCESSING

All data processing activities are carried out exclusively within the EU or the EEA.

7. SUB-PROCESSORS

7.1. The processor may call in sub-processors. He has to inform the controller of the intended use of a sub-processor in a timely manner.

7.2. The processor concludes the necessary agreements with the sub-processor according to Article 28 (4) GDPR. In doing so, it must be ensured that the sub-processor undertakes the same obligations as the processor under this agreement.

8. GENERAL PROVISIONS

In addition, all provisions of the agreements made in point 1 also apply to this agreement.

....

[*Place*], on [*date*] [*place*], on [*date*]

For the controller: *For the processor:*

....

Legal signature *Legal signature*

Initials | | |

Appendix 1

Technical and organizational measures of the processor

1. Entrance control

Measures designed to prevent unauthorized persons from accessing data processing equipment that processes or uses personal data.

☒ Chip card / transponder locking system

2. Admission control

Measures designed to prevent data processing systems from being used by unauthorized persons.

☒ Assignment of user rights ☒ Creating user profiles

☒ Password assignment ☒ Use of VPN technology

☒ Authentication with username / password ☒ Assignment of user profiles to IT systems

☒ Use of intrusion detection systems ☒ Use of a software firewall

☒ Use of anti-virus software

☒ Use of a hardware firewall

3. Access control

Measures to ensure that those entitled to use a data processing system can only access the data subject to their access rights and that personal data can not be read, copied, altered or removed during processing, use and after storage.

☒ Password policy incl. password length, password change

☒ Proper destruction of data carriers (DIN 32757 or ÖNORM S 2109-1)

4. Transmission control

Measures to ensure that personal data can not be illegally read, copied, altered or removed during electronic transmission or during the transport or storage on data carriers, and that it is possible to verify and determine to which places a transfer of personal data is intended by institutions for data transmission.

☒ Set-up of leased lines or VPN-tunnels

☒ For physical transport: careful selection of transport personnel and vehicles

☒ For physical transport: secure transport containers / packaging

Initials | | |

5. Input Control

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data has been entered, changed or removed in data processing systems.

☒ Partial logging of input, modification and deletion of data

☒ Assignment of rights to input, change and deletion of data based on a authorization concept

☒ Partial traceability of input, modification and deletion of data by individual usernames (not user groups)

6. Order control

Measures to ensure that personal data processed on order can only be processed in accordance with the instructions of the customer.

☒ Commitment of the employees of the processor on the data secrecy

☒ Ensuring the destruction of data after the termination of the contract

7. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

☒ Uninterruptible power supply (UPS)

☒ Air conditioning in server rooms

☒ Devices for monitoring temperature and moisture in server rooms

☒ Create a backup & recovery concept

☒ Testing Data Recovery

☒ Storage of data in a safe, outsourced place

8. Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

☒ Logical client separation (software side)

☒ Separation of productive and test system

Initials