Agreement on handling personal data on someone's behalf
(order processing in accordance with Article 28 GDPR)

between

Laboklin GmbH & Co. KG
Steubenstraße 4
97688 Bad Kissingen

(hereinafter referred to as the "**contracting authority**")

and (practice address / stamp)

(hereinafter referred to as the "**contractor**")

1. Object and duration of the order

The object of the order can be derived from the particular services to be commissioned in each case. These are referred to here. The order remains in place until it is terminated by one of the parties.

2. Details regarding order content

(1) Fulfilment by the contractor of the specific activities detailed in the relevant order determines the envisaged scope, nature and purpose of the personal data processing.

(2) The contractually agreed data processing will take place exclusively in a country which is a member of the European Union or in another country which has signed up to the Agreement on the European Economic Area. Any transfer to a third country requires prior approval from the contracting authority and can only take place if the special provisions in Art. 44 ff. GDPR have been met.

3. Types of data

Personal data processing will involve the following categories and types of data:

- contractual and contact data for customers and interested parties, name, address, email address, telephone number, date of birth, delivery address, information on order status, and also data from the contractor's customers relating to payment

- contact data for the contracting authority’s staff and service providers involved, name, address and email address

- communication data (e.g. telephone, email), contract master data (contractual relationship, interest in products or contracts), customer history

4. Data subject categories

The following data subjects are affected by the data processing:

- interested parties
- the contracting authority’s established customers
- the contracting authority’s staff and external service providers who are responsible for fulfilling the aforementioned processing objectives
- customers
- contacts

5. Technical and organisational measures

(1) Before processing begins, the contractor must implement the necessary technical and organisational measures which were outlined before the order was placed, in particular regarding order execution. These measures must be documented and presented to the contracting authority for review. Following acceptance by the contracting authority, the documented measures form the basis for the order. If a review or audit by the contracting authority results in a need to make adjustments, this must be implemented by mutual consent.

(2) The contractor must ensure security in accordance with Art. 28 para. 3(c), 32 GDPR, especially in conjunction with Art. 5 para. 1, para. 2 GDPR. As a whole, the measures to be implemented involve data security measures and steps to ensure an appropriate level of protection, given the relevant risk, for system confidentiality, integrity, availability and resilience. This implementation must take into account the latest technological innovations, implementation costs and the nature, scope and purpose of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons in terms of Art. 32 para. 1 GDPR [details in Annex 1].

(3) The technical and organisational measures are subject to technical developments and enhancements. In this respect, the contractor is permitted to implement adequate alternative measures. The resulting level of security must not fall short of that offered by the established measures. Any significant alterations must be documented.

6. Rectification, restriction and deletion of data

(1) The contractor must not make unauthorised corrections to the data being processed, nor can they delete or restrict the processing of this data. Any such activity requires documented instruction from the contracting authority.

In the event that a data subject contacts the contractor directly in this regard, the contractor will pass on this request immediately to the contracting authority.

(2) Following documented instruction from the contracting authority, and provided this is included in the scope of service, the contractor must immediately ensure compliance with the deletion request, the right to be forgotten or the right to correction, data portability and access.

7. Quality assurance and other contractor obligations

In addition to complying with the provisions in this order, the contractor also has statutory obligations in accordance with Art. 28 to 33 GDPR. In this respect, compliance with the following specifications in particular must be ensured:

(1)

The written appointment of a data protection officer, who will exercise his/her duties in accordance with Art. 38 and 39 GDPR.

Their contact details will be issued to the contracting authority to enable direct contact between the two. Any change to the data protection officer will be communicated immediately to the contracting authority.

The appointed data protection officer for the contractor is Ms Lisa Scheblein, SiDIT GmbH, Unterdürrbacher Straße 8, 97080 Würzburg, info@sidit.de. Any change to the data protection officer must be communicated immediately to the contracting authority.

(2) Maintaining confidentiality pursuant to Art. 28 para. 3(2)(b), 29, 32 para. 4 GDPR. The contractor will only engage staff to carry out the work who have been obliged to maintain confidentiality and who have been made familiar in advance with the data protection provisions which are relevant for them. The contractor and all staff reporting to the contractor who have access to personal data must only process this data in accordance with the instructions from the contracting authority, including the powers conferred in this contract, unless they are obliged under law to process the data.

(3) Implementation and compliance with all technical and organisational measures required for this contract in accordance with Art. 28 para. 3(2)(c), 32 GDPR [details in Annex 1].

(4) On request, the contracting authority and the contractor will work in collaboration with the supervisory authority in fulfilling their responsibilities.

(5) Immediate information for the contracting authority regarding audit activities or other measures by the supervisory authority, insofar as these relate to this order. This also applies if, as part of non-compliance or criminal proceedings, a responsible authority evaluates the contractor’s processing of personal data during order processing.

(6) If the contracting authority itself is subject to a review by the supervisory authority, or to non-compliance or criminal proceedings, or a liability claim from a data subject or third party or to some other claim in conjunction with order processing, the contractor must offer their support to the best of their ability.

(7) The contractor will regularly check its internal processes and the technical and organisational measures in place in order to ensure that processing in their area of responsibility complies with the requirements of the applicable data protection legislation and that the rights of data subjects are protected.

(8) The ability to demonstrate any technical and organisational measures implemented to the contracting authority under its inspection capacity according to clause 9 of this contract.

8. Subcontractor relationships

(1) In terms of this regulation, subcontractual relationships are understood to refer to services relating directly to the principal contractual performance. These do not include ancillary services used by the contractor, e.g. telecommunication services, postal/transport services, maintenance and user services or the disposal of data carriers or any other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software used in data processing facilities. However, the contractor is obliged to put in place appropriate, lawful contractual agreements and inspection measures to ensure that the contracting authority's data is protected and secure even for outsourced ancillary services.

(2) The contractor may only appoint subcontractors (additional processors) following explicit prior written approval or documented authorisation from the contracting authority.

The contracting authority agrees to the appointment of the following subcontractor on condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR:

iWeltAG, Mainparkring 4, 97246 Eibelstadt

(3) Outsourcing to subcontractors or a change to the current subcontractor is permissible, provided the contractor notifies the contracting authority in writing of this outsourcing arrangement a reasonable amount of time in advance, and provided the contracting authority has not notified the contractor in writing of their objection to the proposed outsourcing prior to the time when the data is transferred and a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is put in place on which the arrangement will be based.

(4) All preconditions for subcontracting must be met before it is permitted to pass the contracting authority's personal data on to subcontractors or for them to commence their activities in the first place.

(5) If the subcontractor performs the agreed service outside the EU/EEA, the contractor must ensure that this is permissible under data protection legislation by instigating appropriate measures. The same applies if service providers are to be appointed in terms of para. 1 (2).

9. Contracting authority's supervision rights

(1) The contracting authority has the right to carry out checks on the contractor's conduct or to appoint auditors to carry out such checks in specific cases. The contracting authority is entitled to conduct random inspections, which should generally be announced in good time, to satisfy themselves that the contractor is complying with this agreement in their business operations.

(2) The contractor must ensure that the contracting authority can be persuaded that they are complying with their duties as a contractor under Art. 28 GDPR. The contractor undertakes to provide the contracting authority with the necessary information when requested and, in particular, to demonstrate that they have implemented the relevant technical and organisational measures.

(3) Verification of measures which do not concern the specific order can be provided by complying with an approved code of conduct as per Art. 40 GDPR, or through certification under an approved certification procedure as per Art. 42 GDPR; current certificates, reports or report extracts from independent bodies (e.g.

accountants, auditors, data protection officers, IT security department, data protection or quality assurance auditors) or through appropriate certification from an IT security or data protection audit (e.g. under “BSI Grundschutz” [the German Federal Office for Information Security basic protection audit])

(4) The contractor may demand remuneration in order to facilitate inspections by the contracting authority.

10. **Notification of a breach affecting the contractor**

(1) The contractor will support the contracting authority in complying with their obligations under Articles 32 to 36 of the GDPR concerning the security of personal data, the obligation to report data breaches, data protection impact assessments and prior consultations. This includes:

(a) ensuring an adequate level of security through technical and organisational measures that take into account the circumstances and purpose of the processing activity and also the predicted probability and severity of any possible legal infringements caused by security vulnerabilities, and that enable any relevant infringements to be identified immediately.

(b) the obligation to report any breaches of personal data immediately to the contracting authority

(c) the obligation to support the contracting authority in terms of its duty to inform the data subject and to provide the contracting authority immediately with any relevant information in this context

(d) supporting the contracting authority with their data protection impact assessments

(e) supporting the contracting authority in terms of any prior consultations with the supervisory authority

(2) The contractor may demand remuneration for any support services not included in the performance specification or which cannot be traced back to misconduct on the part of the contractor.

11. **Contracting authority’s powers of authority**

(1) Verbal instructions will be confirmed immediately in writing by the contracting authority.

(2) The contractor must notify the contracting authority immediately, if they believe that an instruction contravenes the data protection provisions. The contractor is entitled to refrain from implementing the relevant instruction until this has been confirmed or amended by the contracting authority.

12. **Deleting data and returning data carriers**

(1) Creating copies or duplicating the data must not be done without the contracting authority’s knowledge. Excluded from this are backup copies, provided these are required to ensure correct data processing, and also any data which is required in order to comply with statutory retention obligations.

(2) After the contractually agreed work has been completed, or earlier at the request of the contracting authority (and no later than when the service agreement comes to an end), the contractor must hand over to the contracting authority all the documents they have obtained along with the output from any processing or usage activities and any databases associated with the contractual relationship; alternatively, with prior

agreement, these items can be destroyed in compliance with data protection requirements. The same applies for test and discarded material. The deletion records must be presented on request.

(3) Documentation which serves as proof that data processing has been done correctly and in line with the contractual agreement must be retained beyond the end of the contract by the contractor in accordance with the relevant retention periods. The contractor can exonerate themselves of this duty by handing over such documentation to the contracting authority at the end of the contractual period.

Other, general

(1) The contractor must notify the contracting authority immediately, if the contracting authority's data is at risk at the contractor due to potential confiscation or seizure, or due to insolvency or settlement procedures or through other circumstances or third-party activities. The contractor will immediately inform all controllers in this context that ownership of the contracting authority's personal data lies with the contracting authority.

(2) Irrespective of the contracting authority's right of instruction under Section 11 of this agreement, any changes or extensions to this agreement or any of its components require written agreement and there must be an explicit indication that this constitutes a change or extension to these conditions. The same also applies if this formal requirement is to be dispensed with.

(3) The provisions in this agreement continue to apply after the primary performance relationship has come to an end and until all of the contracting authority's personal data has either been completely destroyed or returned.

________________________________ ________________________

(place, date) (signature, contracting authority)

_______________________________ _________________________

(place, date) (signature, contractor)

Annex 1:
Technical and organisational measures (TOM)
in terms of Art. 32 GDPR

for the organisation

Laboklin GmbH & Co. KG
Steubenstraße 4
97688 Bad Kissingen

Status

17/05/2018

Organisations which collect, process or use personal data, either themselves or on someone else's behalf, must implement the technical and organisational measures required to ensure compliance with the provisions under data protection legislation. Measures are only required if the effort involved is proportionate given the desired level of protection.

The aforementioned organisation meets this requirement through the following measures:

1. Confidentiality acc. to Art. 32 para. 1 GDPR

1.1. Access control

Measures which are appropriate to deny unauthorised access to data processing systems being used to process personal data. As measures to control access, building and area security could include use of automatic access control systems, chip cards and transponders, controlling access via a gatekeeper service and alarm systems. Servers, telecommunication facilities, network technology and other similar systems must be protected by being located in lockable server cabinets. In addition, it makes sense to support access control through organisational measures (e.g. work instructions to encourage staff to lock office areas in their absence).

Technical measures	Organisational measures
☒ Alarm system	☒ Key control / list
☒ Chip cards / transponder systems	☒ Reception / gatekeeper
☒ Security locks	☒ Visitor book / visitor log
☒ Lock system with code lock	☒ Staff/visitor ID
☒ Doors with external knob	☒ Visitors accompanied by staff
	☒ Care when selecting security personnel
	☒ Care when selecting cleaning services

1.2. Login control

Appropriate measures to prevent data processing systems (computers) from being used by unauthorised persons.
By login control what is meant is preventing unauthorised system use. Possible options include a boot password, user recognition with password for operating systems and software, screen savers with password, use of chip cards to register and also the use of callback procedures. Additional organisational measures may also be necessary; for instance to prevent unauthorised viewing (e.g. specifications for erecting monitors, issuing guidance for users on selecting a "good" password).

Technical measures	Organisational measures
☒ Login with user name + password	☒ Administration of user privileges
☒ Antivirus software server	☒ Central password allocation
☒ Antivirus software clients	☒ "Secure password" guideline

☒ Antivirus software mobile devices	☒ “Deleting/destroying” guideline
☒ Firewall	☒ General guideline on data protection and/or security
☒ Intrusion detection systems	
☒ Use of VPN for remote access	
☒ Automatic desktop locking	

1.3. Permission control

Measures which ensure that those authorised to use a data processing system only have access to data which is governed by their access permissions, and that when personal data is being processed or used and after it has been saved, it cannot be read, copied, modified or removed in an unauthorised manner. One way to ensure this permission control is to have an appropriate user privileges model which allows differentiated access control to all data. This includes both differentiated access to the data itself, but also to the possible functions which can be performed on the data. In addition, appropriate control mechanisms and responsibilities must be defined to document the allocation and withdrawal of permissions and to keep this up to date (e.g. for new staff appointments, work location changes, staff departures). Particular attention must always be paid to the roles and opportunities for administrators.

Technical measures	**Organisational measures**
☒ Paper shredder (at least level 3, cross cut)	☒ Use of permissions concept
☒ External document shredder (DIN 32757)	☒ Minimum number of administrators
☒ Physical deletion of data carriers	☒ Data privacy safe
☒ Logging system access and use, specifically when entering, modifying and deleting data	☒ Managing user permissions via administrators

1.4. Segregation control

Measures which ensure that data which is collected for different purposes can be processed separately. For instance, this can be ensured through logical and physical segregation of data.

Technical measures	**Organisational measures**
☒ Separation of production and test environments	☒ Control of the permissions concept
☒ Multi-client capability for relevant applications	☒ Establishing database permissions

1.5. Pseudonymisation (Art. 32 para. 1(a) GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in a manner which means that the data can no longer be linked with a specific data subject without reference to additional information, provided this additional information is stored separately and is subject to appropriate technical and organisational measures;

Technical measures	**Organisational measures**
☒ As far as possible, pseudonymise data for transfer abroad and/or in general when transferred to a third party	☒ As far as possible, pseudonymise data for transfer abroad and/or in general when transferred to a third party

2. Integrity (Art. 32 para. 1(b) GDPR)

2.1. Transfer control

Measures which ensure that personal data cannot be read, copied, modified or removed in an unauthorised manner during electronic transfer or during transportation or while being stored on data carriers and to ensure that checks can be made to determine where personal data will be sent using data transmission facilities. To ensure confidentiality during electronic data transmission one option is to use encryption technology and virtual private networks. Measures for data carrier transportation or data transfer include transport containers with locking devices and rules for destroying data carriers in compliance with data protection legislation.

Technical measures	Organisational measures
☒ Email encryption	☒ Care when selecting transport, personnel and vehicles
☒ Use of VPN	☒ Personal delivery with record
☒ Logging access and retrievals	
☒ Providing data via encrypted connections such as sftp, https	

2.2. Input control

Measures which ensure that it is possible to determine subsequently whether and by whom personal data was entered, modified or removed on data processing systems. Input controls are achieved using logging mechanisms which can operate at different levels (e.g. operating system, network, firewall, database, application). Here it is also important to clarify what data is being logged, who has access to the log, who will be checking it and at what point or for what reason, how long the log must be retained and when the log will be deleted.

Technical measures	Organisational measures
☒ Technical logging of data input, modification and deletion	☒ Overview of which programs can input, modify or delete which data
☒ Manual or automatic log checking	☒ Ability to trace data input, modification and deletion via individual user names (not user groups)
	☒ Allocation of permissions to input, modify and delete data based on an access control model
	☒ Retention of forms which have supplied data for automated processing

3. Availability and resilience (Art. 32 para. 1(b) GDPR)

3.1. Availability control

Measures which ensure that personal data is protected against accidental destruction or loss. This involves issues such as uninterruptible power supply, air conditioning facilities, fire prevention, data backups, secure storage of data carriers, virus protection, RAID systems, disk mirroring etc.

Technical measures	Organisational measures
☒ Fire alarms and smoke detectors	☒ Backup & recovery concept (formulated in detail)
☒ Server room fire extinguishers	☒ Backup procedure checks
☒ Server room temperature and moisture monitoring	☒ Regular tests on restoring data and logging the results
☒ Air-conditioned server room	☒ Keeping backup media in a secure location outside the server room
☒ UPS	☒ No sanitary connections in or above the server room
☒ Protected power outlet strips server room	☒ Existence of an emergency plan (e.g. BSI IT basic protection 100-4)
☒ RAID system / hard disk mirroring	☒ Separate partitions for operating systems and data

4. Procedure for regular checking, assessment and evaluation (Art. 32 para. 1(d) GDPR; Art. 25 para. 1 GDPR)

4.1. Data protection management

Technical measures	Organisational measures
☒ A check on the efficacy of the technical security measures will be carried out at least once per year.	☒ Internal / external data protection officer name / company / contact data
	☒ Staff trained and required to maintain confidentiality / data secrecy
	☒ Regular awareness raising campaigns for staff, at least annually

4.2. Incident response management

Support for response to security breaches

Technical measures	Organisational measures
☒ Use of a firewall and regular updates	☒ Documentation of security incidents and data breaches e.g. via ticket system
☒ Use of spam filter and regular updates	
☒ Use of virus scanner and regular updates	

4.3. Privacy-friendly default settings (Art. 25 para. 2 GDPR)

Privacy by design / privacy by default

Technical measures
☒ No personal data is collected beyond what is required for the relevant purpose.
☒ Straightforward option for data subjects to exercise their cancellation right via technical measures

4.4. Order control (outsourcing to third parties)

Measures which ensure that personal data being processed on someone else's behalf can only be processed in accordance with the contracting authority's instructions. Along with outsourced data processing, this item also includes maintenance and system support work carried out either on site or via remote servicing. If the contractor engages service providers to assist with order processing, agreement on the following items should always be established with these service providers.

Organisational measures
☒ Contractor selection with careful consideration (especially in relation to data protection and security)
☒ Putting in place the necessary agreement on order processing or standard EU contractual terms
☒ Written instructions to the contractor
☒ Requiring the contractor's staff to maintain data confidentiality

Completed for the organisation by

Name	Dr Claudia Simon / Mr Michael Atzler
Role	Vet/QM officer / administrator
Phone number	0971 / 72020
Email	simon@laboklin.com

Location, Date Bad Kissingen, 17/05/2018