

Agreement on the contract processing of personal data in WiredMinds LeadLab in accordance with GDPR

Please send the signed contract to
datenschutz@wiredminds.de

The team of WiredMinds GmbH

Phone: 0049 711 585 331 0
E-mail: datenschutz@wiredminds.de
Web: www.wiredminds.de

Contracting parties

Contractor

Principal (please enter data)

WiredMinds GmbH

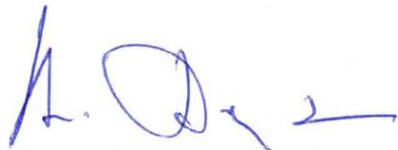
Lindenspürstr. 32

D-70176 Stuttgart

Represented by:

Represented by: (Please enter data)

Place, Date



Albert Denz
Managing Director

1 Introduction, Scope of Application, Definitions

- (1) This Agreement regulates the rights and obligations of Principal and Contractor (hereinafter referred to as the “Parties”) within the context of contract processing of personal data.
- (2) This Agreement applies to all activities in which employees of the Contractor or subcontractors which the Contractor has commissioned (Subcontractors) process personal data.
- (3) Terms used in this Agreement shall be understood in accordance with their definition in the EU General Data Protection Regulation. If in the following explanations have to be made in “writing”, the written form pursuant to Section 126 of the German Civil Code (BGB) is meant. In all other cases, explanations may be given in a different form provided that suitable proof can be guaranteed.
- (4) With your signature, you confirm that you acknowledge this “Agreement on the contract processing of personal data in WiredMinds LeadLab in accordance with GDPR” without modifications (with the exception of Item 2).

2 Subject matter and duration of the processing

2.1. Subject matter

Subject matter, nature and extent as well as the purpose of the data processing arise from the main agreement concluded between the owner of the data and the contracting party.

Name of the main agreement:

Date of concluding the Agreement:

2.2. Duration

The processing shall commence on

Starting date of the project / start of the test account:

and shall take place for an indefinite time until termination (Item 11) of this Agreement or the Main Agreement by one Party.

3 Nature and purpose of the data capture, processing or use:

3.1. Nature and purpose of the use

The nature of the processing is as follows:

collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, making available, alignment, restriction, erasure or destruction of data

The purpose of the processing is as follows:

WiredMinds LeadLab records the data of visits to the Principal's domain and evaluates the data of identified visits by companies. During this process, the user behaviour is analysed in order to recognize a possible focus of interest on the part of the user.

The recorded data will be made available to the Principal in a cloud-based software solution. In addition, individual employees of WiredMinds shall have access to these data so as to be able to implement topics from the field of support, service, development. The data will also be stored with our hosting partner. No access rights to the data exist here with respect to the employees of our hosting partner.

3.2. Nature of the data

The types of data collected during use of the software include the following:

- User identifiers and user master data of the Principal's employees (software users)
- User usage data of the Principal's employees in the form of log files (service monitoring and security)
- Hosting of CRM data, which may also be personal such as notes

The following types of data are collected from the recorded visitors to the website:

- IP address of the website visitor
The IP address is not stored in this process. The IP address is used merely to filter out natural persons to facilitate their protection.

3.3. Categories of data subjects

Processing affects:

- Employees of the Principal (users of LeadLab)
- Visits (legal persons) to the Principal's website

4 Duties of the Contractor

- (1) The Contractor shall process personal data exclusively as agreed by contract or as instructed by the Principal unless the Contractor is legally obliged to perform a certain type of processing. Moreover, the Contractor shall use personal data made available for the processing for no other purposes, particularly his own.
- (2) The Contractor confirms that he is familiar with the relevant, general data protection regulations.
- (3) The Contractor undertakes to strictly preserve the confidentiality of the data during the processing.
- (4) Persons who may obtain knowledge of the personal data processed in the order shall undertake in writing to maintain confidentiality to the extent that they are not already legally subject to a relevant secrecy obligation.
- (5) The Contractor gives his assurance that the persons deployed for processing have been made familiar with the provisions of data protection and of this Agreement before commencement of the processing. Appropriate training and awareness measures shall be repeated with appropriate regularity. The Contractor shall ensure that persons deployed for processing the order are continuously instructed and monitored with respect to fulfilment of the data protection requirements.
- (6) In connection with the commissioned processing, the Contractor shall support the Principal in preparing and continuing the directory of processing activities as well as in conducting the data protection impact assessment. The details and documents required for this shall be maintained and forwarded to the Principal on request without undue delay.
- (7) If the Principal is subjected to an inspection by supervisory authorities or other entities or if data subjects assert their rights over the Principal, the Contractor undertakes to support the Principal to the necessary extent in as far as the processing is affected within the order.
- (8) The Contractor may only give information to third parties or the data subject after prior consent of the Principal has been obtained. The Contractor shall forward any requests addressed directly to him to the Principal without delay.
- (9) Insofar as he is legally obliged, the Contractor shall appoint a qualified and reliable person as officer for data protection. It must be ensured that the officers have no conflicts of interest. In cases of doubt, the Principal may contact the data protection officer directly. The Contractor shall supply the Principal with the contact data of the data protection officer without delay or will provide reasons why no officer has been appointed. The Contractor shall notify the Principal of any changes in the person or the in-company tasks of the officer without delay.
- (10) The contract processing shall take place exclusively within the EU or the EEA. Any relocation to a third country may only take place with the consent of the Principal and under the conditions contained in Chapter V of the General Data Protection Regulation and pursuant to the provisions of this Agreement.

5 Technical and organisational measures

- (1) The data security measures described in Annex 1 are specified as binding. They define the minimum demand from the Contractor.
- (2) The data security measures may be adapted in accordance with further technical and organizational development as long as they do not fall below the level agreed here. The Contractor shall implement any changes required to maintain information security without delay. The Principal shall be notified of any changes without delay. The Principal has the right to object in writing to a change in the technical and organizational measures, informing the Contractor of the reasons for the objection, within a period of 4 weeks. If no objection is submitted, the change is deemed to have been approved.
- (3) If the security measures taken do not meet or no longer meet the Principal's requirements, the Contractor shall inform the Principal without delay.
- (4) The Contractor guarantees that the data processed under contract are strictly separated from any other data stocks.
- (5) Copies and duplicates shall not be made without the knowledge of the Principal. Exceptions to this are technically necessary, temporary duplicates, provided that any impairment of the agreed level of data protection is ruled out.
- (6) The processing of data in a home office is permissible provided the employee concerned has concluded the currently valid home office agreement with the employer (Contractor). If such processing takes place, the Contractor shall ensure that the a level of data protection and data security corresponding to this Agreement is maintained and that the Principal's control specified in this Agreement can also be exercised without any restriction in the private dwellings affected. The contract processing of data with private devices is not permitted under any circumstances.
- (7) The Contractor shall provide regular evidence of compliance with his duties, in particular the complete implementation of the agreed technical and organizational measures. This evidence can be made available at any time at the request of the Principal. The evidence may be provided through approved rules of conduct or an approved certification procedure.

6 Regulations on the correction, erasure and blocking of data

- (1) The Contractor shall only correct, erase or block data processed within the scope of the order in accordance with the contractually made Agreement or following instructions from the Principal.
- (2) The Contractor shall follow the corresponding instructions from the Principal at all times and also beyond the termination of this Agreement unless the instructions are unlawful, do not comply with the provisions of this Agreement or are actually impossible for the Contractor to fulfil.

7 Subcontractual relations

- (1) The Principal agrees that the Contractor may call in subcontractors. The Principal shall be notified in writing of each individual case of commissioning subcontractors, i.e. of any intended change in relation to the enlistment or replacement of other subcontractors. The Principal has the right to object in writing to a subcontracting of activities within 4 weeks and by stating the reasons. If no objection is submitted, the enlistment of the subcontractor is deemed to have been approved. The Principal may give written notice of the approval at any time. Prior to approval, the subcontractor will not be given access to any data for contract processing. If it is not possible to reach mutual agreement between the parties in relation to the reasons for objection, both parties shall be entitled to extraordinary termination of this Agreement and the Main Agreement.
- (2) The award of a contract to subcontractors must take place in writing. The Contractor shall select the subcontractor carefully. Prior to the start of data processing by the subcontractor and then at regular intervals, the Contractor shall satisfy himself that the technical and organizational measures taken on the part of the subcontractor are observed and shall document the results. A copy of the order as well as the inspection documentation shall be made available to the Principal on request.
- (3) If subcontractors are enlisted by the Contractor, the contractual agreements shall be designed in such a way as to comply with the requirements of this Agreement. The Principal shall be granted rights of control and inspection pursuant to Section 8 of this Agreement. The Principal is similarly entitled on issuing a written request to obtain information on the essential contents of the contract and the implementation of the subcontractor's obligations relevant to data protection, if required also through access to the relevant contractual documents.
- (4) If the subcontractor originates from outside a Member State of the European Union or in another signatory state to the Agreement on the European Economic Area or the data processing takes place there, the Contractor shall additionally ensure that the conditions stated in Chapter 4 (10) are observed. The Principal shall be provided with written proof of this before the subcontractor commences its activities.

8 Rights and obligations of the Principal

- (1) The Principal is solely responsible for assessing the permissibility of the commissioned processing as well as for safeguarding the rights of those affected.
- (2) The Principal shall document the issue of all orders, partial orders or instructions. In urgent cases, instructions may be given orally. The Principal shall confirm such instructions in documented form without delay.
- (3) The Principal shall inform the Contractor without delay if he detects errors or irregularities during the inspection of the results of the order.
- (4) To a reasonable extent, the Principal is entitled to monitor the adherence to regulations governing data protection and the contractual agreements at the Contractor's premises himself or through third parties, in particular by gathering information and inspection of the stored data and the data processing programs as well through other on-site examinations. The person entrusted with monitoring shall be granted access and viewing rights to the extent required. The Contractor is obliged to provide the necessary information, demonstrate processes and maintain records as necessary to conduct an inspection.
- (5) Inspections at the Contractor's premises shall take place without any avoidable disruptions to the operation of his business. Unless otherwise indicated by urgent reasons to be documented by the Principal, inspections shall take place after appropriate advance notice has been given and during the Contractor's business hours and not more often than every 12 months. Provided the Contractor provides proof that the agreed data protection obligations have been implemented, as provided for under Chapter 5 (8) of this Agreement, an inspection shall be limited to random samples.

9 Notification obligations

- (1) The Contractor shall notify the Principal of any personal data breaches without undue delay. Notification shall also be given in any cases of justified suspicion. The notification shall at least contain the details pursuant to **Art. 33 para. 3 of the General Data Protection Regulation**.
- (2) Notification without undue delay shall also be given of any substantial disruptions to the execution of the contract processing as well as any violations by the Contractor or by persons employed by him of the provisions under data protection law or the specifications laid down in this Agreement.
- (3) The Contractor shall inform the Principal without undue delay of inspections or measures by supervisory authorities or other third parties insofar as they are related to the contract processing.
- (4) The Contractor undertakes to provide support to the Principal to the extent required with his duties pursuant to Art. 33 and Art. 34 of the General Data Protection Regulation.

10 Instructions

- (1) The Principal reserves comprehensive instruction rights in respect of the contract processing.
- (2) Principal and Contractor shall appoint the persons exclusively authorized to issue and receive instructions in Annex 3.
- (3) If the appointed persons should be changed or hindered for a lengthy period of time, the other party shall be notified of successors or substitutes.
- (4) The Contractor shall without undue delay draw the Principal's attention to any instructions issued by the Principal which in the Contractor's opinion are in breach of statutory regulations. The Contractor is entitled to suspend the execution of the relevant instruction until it has been confirmed or amended by the person responsible on the part of the Principal.
- (5) The Contractor shall document all the instructions issued to him and their implementation.

11 Termination of the contract

- (1) On termination of the contractual relationship or at any time when requested by the Principal, the Contractor shall either destroy or hand over to the Principal, in accordance with the Principal's choice, the data processed under contract. All existing copies of the data shall also be destroyed. The destruction shall be performed in such a way that recovery even of residual information shall no longer be possible with reasonable expense and effort. Physical destruction shall take place in accordance with DIN 66399. Protection category 3 shall apply as a minimum.
- (2) The Contractor is also obliged to arrange for the immediate return or erasure on the part of subcontractors.
- (3) The Contractor shall keep a record of the proper destruction and shall present this to the Principal without undue delay.
- (4) Documentation recording the proper processing of the data shall be retained by the Contractor in accordance with the respective storage periods beyond the end of the Agreement as well. To reduce his duties, he may hand them over to the Principal on termination of the Agreement.

12 Liability

- (1) Principal and Contractor shall assume joint and several liability to render compensation for damages suffered by a person on account of prohibited or incorrect data processing within the scope of the contractual relationship.
- (2) The Contractor shall be liable to the Principal for any culpable damage caused by the Contractor, his employees or the persons deployed to execute the Agreement or the enlisted subcontractors in connection with providing the commissioned contractual service.
- (3) Paragraph (2) shall not apply if the damage has arisen due to the correct implementation of the commissioned service or an instruction issued by the Principal.

13 Right to extraordinary termination

- (1) The Principal may terminate this Agreement at any time without notice ("extraordinary termination") if the Contractor has seriously violated the data protection regulations or the provisions of this Agreement, the Contractor is unable or unwilling to execute a lawful instruction from the Principal, or the Contractor is in breach of contract by refusing to follow the Principal's controlling rights.
- (2) A serious violation shall apply in particular if the Contractor does not fulfil or has not fulfilled the agreed technical and organizational measures specified in this Agreement to a substantial extent.
- (3) In the case of insubstantial violations, the Principal shall set the Contractor a reasonable period of notice for remedial action. If the remedial action does not take place in time, the Principal shall be entitled to extraordinary termination, as described in this Section.

14 Miscellaneous

- (1) Both parties undertake to treat all knowledge of business secrets and data security measures of the respective other party in strict confidence even beyond termination of the Agreement. Should any doubt exist as to whether an item of information is subject to the duty of confidentiality, it shall be treated as confidential until written release has been provided by the other party.
- (2) Should any property of the Principal located with the Contractor be at risk on account of measures by third parties (e.g. seizure or confiscation), insolvency or composition proceedings or other events, the Contractor shall inform the Principal without delay.
- (3) The written form is required for any ancillary arrangements.
- (4) The defence of right of retention as defined by Section 273 of the German Civil Code (BGB) is excluded with reference to the data processed in the contract and the associated data storage media.
- (5) Should any individual parts of this Agreement be invalid, this shall not affect the remaining regulations in the agreement.

15 Annexes

Annex 1: Description of the technical and organizational measures

Annex 2: Contractor's data protection officer

Annex 3: Issuers and recipients of instructions

Annex 4: Subcontractors engaged

Annex 1

Technical and organizational measures for the security of data processing

The following describes which technical and organizational measures are defined for guaranteeing data protection and data security. The objective is to guarantee in particular the confidentiality, integrity and availability of the information processed in the company. The structure is oriented towards the internationally recognized standard DIN ISO/IEC 27002.

01. Guideline

The data protection guideline of WiredMinds GmbH contains the key statements by the management on handling personal data within the company. All employees, freelancers and supporting companies are obliged to observe these key regulations. The level of IT security achieved by the organizational units, processes and systems is monitored by a combination of periodically recurring inspections and continuous controls.

Inspections of ongoing operations shall take place in consultation with the security officer. A review of the security policy shall take place at least once per year unless an essential change makes this necessary at an earlier date.

This ensures the continuing appropriateness, suitability and effectiveness of the regulation. The security officer is the person accountable for the security policy and is responsible for its development, revision and inspection.

02. Organization of information security

The management staff of WiredMinds GmbH are responsible for the complete implementation of the principles of IT security within their organizational unit and for fulfilling the security tasks demanded of them.

Information security roles and responsibilities are defined in the IT security organization. Conflicting tasks and areas of responsibilities are separated in order to reduce the opportunities for unauthorized or unintended modification or misuse of our company's assets.

We have a procedure that defines when and by whom relevant authorities are notified and detected data protection and information security incidents are reported in a timely manner. We also maintain regular contact with special interest groups in order to remain informed of changes and improvements in the field of data protection and information security.

Within our projects, data protection and data security are a constituent part of all phases of our methodology. Through our respective guidelines and processes on teleworking and the usage of mobile devices, we also ensure data protection and data security in these areas as well.

Annex 1

Technical and organizational measures for the security of data processing

03. Personnel security

We have selected our employees carefully and examined their suitability for their role within the company. We have laid down their responsibilities in functional job descriptions and conduct regular comparisons as to whether the employees comply with them. Prior to their appointment, all employees sign a confidentiality and data protection agreement that applies beyond the end of their employment relationship. The employees are trained in the field of data protection and data security, in particular refreshment training sessions take place again in the event of a functional change. As a result, they are aware of their responsibility in this respect.

In a documented process for the period before, during and after termination of the employment relationship, we ensure that personal data are protected and that data security is guaranteed. This also includes disciplinary measures in the event of data protection breaches.

04. Management of assets

All assets (e.g. operating equipment, notebook computers, smartphones) and information connected with personal data are recorded and maintained by us in an inventory.

To protect these assets, we have specified controllers who are responsible for the life cycle of an asset.

Documented regulations have been established for the permissible use of our assets. Their return is documented.

Our information and data are classified and identified using the statutory requirements, their value, their criticality and their sensitivity to unauthorized disclosure or amendment.

In accordance with this classification scheme, we have developed and implemented documented procedures for the handling of our assets. We do not normally transfer data on removable storage media but instead exclusively in encrypted form via verified communication channels. Deviations from this practice are only possible in exceptional cases on the written instruction of the client.

We securely dispose of any data storage media no longer required using a documented procedure and contractually bound certified service providers.

Annex 1

Technical and organizational measures for the security of data processing

05. Access control

We have regulated and documented measures which ensure that authorized persons only obtain access to the specific personal data for which they possess consultation and processing powers.

Authorizations for access to IT systems are issued via a regulated procedure based on a documented and restrictive authorization concept. We have regulated and implemented the access to networks and network services.

It is guaranteed that only authorized users have access to systems and services and that unauthorized access is prohibited, in particular a formal process is in place for the registration of users, which enables the allocation of access rights.

The issuing of our administrative rights is limited and controlled.

We have a documented and regulated process for the handling of passwords.

The actual and target status of user access rights are regularly examined and compared. They are withdrawn or adapted as required.

We restrict the access to our data according to needs and control the access to our systems and applications by means of a secure login procedure. We employ a system for using secure and strong passwords.

The use of tools that might be capable of circumventing measures to protect systems and applications is restricted and subject to strict surveillance.

06. Cryptography

The appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information is guaranteed. For this purpose, we have implemented a guideline on the use of cryptographic measures within the company which also encompasses the management of cryptographic keys and is appropriate for the protection requirements.

Annex 1

Technical and organizational measures for the security of data processing

07. Physical and environmental security

We have taken documented and regulated measures that are intended to prevent unauthorized persons obtaining access to data processing systems with which personal data are processed or used. These include:

- The business premises are located in the 3rd storey of an office building and used exclusively
- The central entrance is kept under surveillance
- Doors to security areas are permanently closed
- Visitors or external service providers are admitted individually
- Fire protection is observed by our Hosting Partner
- Security areas exist to which only specially authorized persons have access
- IT rooms are locked separately and can only be opened by authorized persons
- Supply facilities are protected against power outages and disruptions
- Due account is given to the security of cabling
- Systems maintenance is planned and implemented
- The removal and modification of systems and information are regulated
- Due consideration is given to the security of systems outside of the business premises
- The disposal or reutilization of operating resources is regulated
- Unsupervised user devices are protected by an automatic screen saver and automatic hard drive encryption
- Guidelines for a clean desk policy and screen locks are implemented

Annex 1

Technical and organizational measures for the security of data processing

08. Operational safety

We have regulated and documented measures to ensure a proper and secure operation of facilities for processing information and data. These include control in the event of a change to the information-processing facilities as well as the control and regular measurement of our capacities and resources in order to safeguard the availability of the required system performance. Consequently, examples of the values subject to ongoing monitoring include the following:

- Hard disk status and available memory
- Raid status
- Services and status of all virtual machines
- Failed login attempts
- Memory mapping for the storage and main memory
- Capacity utilization of Ethernet
- Number of RDP sessions of the individual terminal servers
- Throughput and capacity utilization of the firewall
- Accessibility of all servers via monitoring
- Accessibility and throughput of the switches

A protected procedure for data backups has been implemented by us and is documented. Standard maintenance windows are defined. Any additional windows required are announced at least 10 days in advance.

It is essential within our company to separate development, test and operating environments from one another so that we pay particular attention to this aspect.

Measures of detection, prevention and recovery for protection against malicious software have been taken and are regularly updated.

We have centrally monitored and protected event logging and have taken measures to protect the private sphere if sensitive personal data have to be stored. All logging facilities and logging information, including administrator and operator logs are protected against manipulation and unauthorized access.

The synchronization of our clocks takes place centrally with one single reference time source.

We have a central procedure for the controlled installation of software on systems within our company.

Annex 1

Technical and organizational measures for the security of data processing

A list of our technical assets exists along with regulated, documented instructions for handling any technical vulnerability that may occur, which includes our patch management with defined responsibilities.

Regulations for restrictions to software installations have been implemented by us centrally.

In the event of our information systems being audited, we have laid down measures to minimize disruptions to business processes as far as possible.

09. Communication security

The security of our personal data and information stored in networks and network services is absolutely essential. We have therefore taken documented measures to manage, control and secure our networks.

Information services, users and information systems are maintained separately from each other in line with demand.

We have guidelines and procedures for the transmission of information and data, as well as agreements for the transmission of information to external locations. (for example CRM-Vendors)

Our electronic messaging is suitably protected. Accordingly, we have taken other measures to protect the messages against unauthorized access, modification or denial of service, which comply with the classification scheme adopted by the organization. (protection class 1_E2)

In order to protect our data, we conclude confidentiality or non-disclosure agreements according to needs, which we regularly review.

Annex 1

Technical and organizational measures for the security of data processing

10. Procurement, development and maintenance of systems

It is guaranteed that the security of data and information is a permanent constituent throughout the entire lifecycle of our systems. This also includes the requirements on and safeguarding of information systems that provide services via public networks. The protection of transactions for application services takes place according to needs. Furthermore, we have set up a procedure for managing system changes in order to secure the integrity of the system, the applications and the products from the early draft phases through to all subsequently occurring maintenance operations.

During changes to operating platforms, applications critical to business are inspected and tested to ensure that there are no negative effects on the organizational security or also on customer applications. We have a controlled process for the analysis, development and maintenance of secure IT systems.

Acceptance test programs and associated criteria are defined for new information systems, updates and new versions. Our test data are carefully selected, protected and controlled.

11. Supplier relationships

We select our suppliers carefully in advance and verify their suitability with respect to safeguarding data and information security protection.

Documented agreements secure the protection and secrecy of our assets and data. The suppliers are obliged to take technical and organizational measures in order to ensure this.

A regulated and user-defined system of access authorization is in place with respect to the assets and data that are absolutely necessary for the respective supplier.

Suppliers may only commission other suppliers with our approval in order to guarantee a secure supply chain.

We regularly conduct a review of the data protection and data security measures of suppliers in order to maintain the agreed level. The authorizations allocated are also subject to continuous documented monitoring.

After termination of the supplier relationship, the suppliers are obliged to destroy the data and assets received from us. Moreover, the obligation to maintain secrecy applies indefinitely.

Annex 1

Technical and organizational measures for the security of data processing

12. Management of information security and data protection incidents

Our company has a regulated and documented process for the handling of information security and data protection incidents in order to ensure a consistent and effective approach in this respect. Employees are bound to report all data protection and security incidents without undue delay and undergo regular training in this respect. We have installed a reporting system that forwards events to an intervention team in order to ensure a rapid reaction. All incidents are documented, classified and evaluated. The intervention team implemented has precise specifications on how to react to an incident.

Improvement measures resulting from the knowledge and accumulated evidence from an incident are regularly discussed with the management and implemented.

13. Aspects of information security in business continuity management

Within the framework of information security, the intended availability of a system is separately evaluated and documented. From the requirements, we derive the technical and organizational specifications such as redundant systems / connections or appropriate plans and implement these in a systematic and controlled manner.

An overarching emergency plan forms the framework in respect of the corresponding instructions for selected documented emergency scenarios.

Regular updated practice schedules for trials of the measures taken and documentation of the performance of corresponding tests round off the emergency management. All server and storage system are rented from a selected computing centre. The contractual agreements mean that a permanent claim to availability is placed on the service provider.

Annex 1

Technical and organizational measures for the security of data processing

14. Compliance

We have specified and documented all relevant, statutory, regulatory, self-imposed or contractual requirements as well as our company's procedure for observing these requirements and keep these regulations and this procedure up to date.

Suitable procedures have also been implemented to ensure adherence to statutory, regulatory and contractual requirements in respect of intellectual property rights and the use of copyright-protected software products.

In accordance with the statutory, regulatory, contractual and business requirements, we protect recordings and personal data in line with needs. Annual reports on the activity of the data protection officer document the measures taken.

We observe the regulations of cryptographic measures in this respect.

To ensure the protection of our information and data, an independent review is conducted regularly of our information security and data protection level, our security and data protection guidelines and the observation of technical specifications.

Annex 2

The **Data Protection Officer** appointed for the Contractor is:

Data protection officer for WiredMinds GmbH
c/o activeMind
Potsdamer Straße 3
D-80802 München

Tel.: +49 (0)89 418 56 01-70
Fax: +49 (0)89 418 560 179
www.activemind.de

E-Mail: datenschutzbeauftragter@wiredminds.de

Records of Processing Activities

WiredMinds GmbH maintains a list of processing activities that comply with legal requirements. This has been approved by the data protection officer of WiredMinds GmbH.

Confidentiality:

All employees of WiredMinds are bound by their employment contract to maintain full confidentiality

Training:

The employees of WiredMinds undergo training, for which records are kept, and are familiar with the issues of data security and data protection

Annex 3

Persons authorized to issue instructions on the part of the Principal are:

1. Authorized Person

First name, Surname or function of person

Phone

E-Mail

2. Authorized Person (optional)

First name, Surname or function of person

Phone

E-Mail

Persons authorized to receive instructions on the part of the Contractor are:

Nicole Widmann

E-Mail: nicole.widmann@wiredminds.de

Phone: 0711 – 585 331 310

Data Protection Officer

E-Mail: datenschutz@wiredminds.de

Tel.: 0711 – 585 331 375

Annex 4

The following subcontractors are currently being deployed to fulfil the order

Hetzner Online AG

Industriestr. 25

91710 Gunzenhausen
Germany

Note:

Technical service provider; purchase of root servers.

There is NO opportunity for the service provider to access data processed under contract.