

Contract about the Order processing of personal data in WiredMinds LeadLab according to DSGVO

Please send the signed contract to
datenschutz@wiredminds.de

Your team at WiredMinds GmbH

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

Introduction

Our LeadLab software complies with all the requirements of the GDPR. WiredMinds and its solutions comply with all data protection rules and regulations. We guarantee this - always and especially today.

Measuring the reach of your website by using WiredMinds LeadLab does not require the consent of your website visitors. Not only we say this, but also the State Office for Data Protection and Information Security, which is responsible for us.

<https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/>

Reason

- We do not collect and store any data on the end user's terminal equipment (§ 25 TTDSG).
- We collect the IP address of the website visitor from the TCP/IP protocol.
- The IP address is used for a one-time, temporary comparison against our company database.
- This process is based on Art. 6 para. 1 (f) DSGVO.
- Only after successful comparison against our company database do we collect visitor data.
- User focus is on determining B2B-relevant website visitors.
- We keep your data in Germany
- We comply with all laws and regulations of the DSGVO

For reach measurement on your behalf, we need this Data protection Addendum because,

- we act on your behalf and carry out reach measurement for your website
- we set up LeadLab access data for you and process your employees' personal data in the process
- we give you the possibility to set up reports in LeadLab, which you can send to an e-mail address (personal value) of your sales employees
- More information and documents can be found at:
- wiredminds.com/privacy or write directly to datenschutz@wiredminds.de

"With WiredMinds, you take no risks. Your data is only your data and its processing is secure and documented. This has always been the case and also applies in the context of the GDPR".

Albert Denz, CEO
WiredMinds GmbH

Contractors

Contractor

Client (please enter data)

WiredMinds GmbH

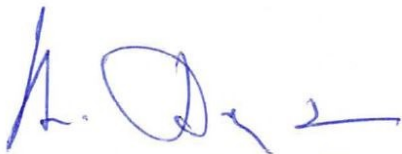
Lindenspürstr. 32

70176 Stuttgart

Represented by

Represented by (please enter data)

City, date



Albert Denz
CEO

1 Subject and duration of processing

1.1. Subject

The subject, type and scope as well as the purpose of the data processing result from the main contract concluded between the Data Controller and the Contractual Partner:

Contract name

Please transfer the corresponding product name "Testaccount"
"LeadLab Lite" "LeadLab" into the field

Date of conclusion of the contract

1.2. Duration

Processing begins on

Please enter the desired start of the contract or the start of the
test phase in the field:

and shall be for an indefinite period of time until termination (Item 10) of this Agreement or the Main Agreement by either Party.

2 Type and purpose of data collection, -processing or -use

2.1. Type and purpose of use

The processing is of the following nature:

Use of WiredMinds GmbH's pixel-counting technology on the client's website to record the IP address of all website visitors and a one-time temporary comparison of the IP address against WiredMinds GmbH's company database. Ordering and sorting the visits according to B2B-relevant visits and filtering out all visits from natural persons. The IP address is not stored, adjusted or changed. The visit behavior of the B2B-relevant companies is recorded, made available to the client in LeadLab and can be used for reach measurement by the client.

Translated with www.DeepL.com/Translator (free version)

The processing serves the following purpose:

- Detection and filtering of potentially identifiable website visitors.
- Maintenance of the provided solution incl. administration of the users at the customer's site

2.2. Type of data

When using the software, the following types of data are collected, among others:

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

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

- IP address of the website visitor

2.3. Categories of data subject

The following are affected by the processing:

- Employees of the client (users of LeadLab)
- Website visitors

3 Duties of the contractor

(1) The Contractor shall process personal data exclusively as agreed or instructed, unless there is a legal obligation to process.

(2) The Contractor undertakes to strictly maintain confidentiality during processing and to obligate assigned employees accordingly.

(3) The Contractor shall support the Customer in the fulfillment of obligations under data protection law or in the context of controls, for example by supervisory authorities, to the extent necessary.

(4) The Contractor may only provide information with the consent of the Customer. The Contractor shall forward any inquiries addressed to it to the Customer.

(5) To the extent required by law, the Contractor shall appoint a competent and reliable person as data protection officer.

(6) The commissioned processing shall take place exclusively within the EU or the EEA. Any relocation to a third country may only take place under the conditions contained in Chapter V of the General Data Protection Regulation.

4 Technical and organizational measures

- (1) The data security measures implemented by the Contractor are described in Annex 1.
- (2) The data security measures may be adapted in accordance with further technical and organizational development as long as the level agreed here is not undercut.
- (3) The Contractor warrants that the data processed in the order will be strictly separated from other data files. Copies or duplicates shall not be made without the knowledge of the Customer. Technically necessary, temporary duplications are excepted.
- (4) The processing of data in the home office is permissible. The Contractor shall ensure that data security is not impaired and that the Customer's control rights can be exercised without restriction.
- (5) The Contractor shall provide regular evidence of the fulfillment of its obligations.

5 Regulations for the correction, deletion and blocking of data

- (1) The Contractor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement reached or in accordance with the Client's instructions.

6 Subcontracting relationships

- (1) The Customer agrees that the Contractor may engage subcontractors. The commissioning of subcontractors, i.e. any intended change with regard to the involvement or replacement of other subcontractors, shall be notified to the Customer in writing in each individual case. The Customer shall have the right to object to a subcontracting within 4 weeks in writing, stating the reasons. If no justified objection is made, the use of the subcontractor shall be deemed approved. If an amicable solution regarding the justification of the objection is not possible between the parties, both parties shall be entitled to extraordinary termination of this contract and the main contract within 14 days.
- (2) The award of contracts to subcontractors shall be made in writing. The Contractor shall carefully select the subcontractor.

7 Rights and obligations of the client

- (1) The Customer shall be solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
- (2) The Customer shall issue all orders, partial orders or instructions in documented form. In urgent cases, instructions may be issued verbally. The Customer shall immediately confirm such instructions in a documented manner.
- (3) The Customer shall inform the Contractor without delay if it discovers errors or irregularities in the examination of the order results.
- (4) The Customer shall be entitled to monitor the Contractor's compliance with the provisions on data protection and the contractual agreements to a reasonable extent itself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site checks. The persons entrusted with the control shall be granted access and inspection by the Contractor to the extent necessary. The Contractor shall be obliged to provide the necessary information, to demonstrate processes and to provide evidence required to carry out a control.
- (5) Inspections at the Contractor's premises shall be carried out without any avoidable disruptions to its business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall take place after reasonable advance notice and during the Contractor's business hours, and not more frequently than every 12 months. Insofar as the Contractor provides evidence of the correct implementation of the agreed data protection obligations, checks shall be limited to random samples. shall be limited to spot checks.

8 Obligations to notify

- (1) The Contractor shall notify the Customer without undue delay of violations of the protection of personal data.
- (2) The Contractor shall inform the Customer without undue delay about controls or measures by supervisory authorities or other third parties, insofar as these are related to the commissioned processing.

9 Instructions

- (1) The Customer reserves a comprehensive right to issue instructions with regard to processing on behalf of the Customer.
- (2) The Contractor shall notify the Customer without undue delay if, in its opinion, an instruction issued by the Customer violates statutory provisions. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or changed by the responsible person at the Customer.

10 Termination of the order

- (1) Upon termination of the contractual relationship or at any time upon request of the Customer, the Contractor shall, at the Customer's option, either destroy the data processed in the order or hand it over to the Customer.
- (2) Documentation which serves as proof of proper data processing shall be retained by the Contractor in accordance with the respective retention periods even beyond the end of the contract. The Contractor may hand them over to the Customer at the end of the contract to relieve the Customer.

11 Liability

- (1) The Contractor shall be liable to the Customer for damage culpably caused by the Contractor, its employees or the subcontractors engaged by it to perform the contract or the subcontractors engaged by it in connection with the performance of the contractual service commissioned.
- (2) Number (1) shall not apply insofar as the damage was caused by the correct implementation of the commissioned service or an instruction issued by the Customer..

12 Other

- (1) Both parties are obligated to treat all knowledge of business secrets and data security measures of the respective other party obtained within the framework of the contractual relationship as confidential, even after termination of the contract. If there is any doubt as to whether information is subject to the obligation of confidentiality, it shall be treated as confidential until it has been released in writing by the other party.
- (2) If property of the Customer with the Contractor is endangered by measures of third parties (for example by attachment or seizure), by insolvency or composition proceedings or by other events, the Contractor shall notify the Customer without delay.
- (3) Additional agreements must be made in writing.
- (4) The defense of the right of retention within the meaning of Section 273 of the German Civil Code (BGB) shall be excluded with respect to the data processed in the order and the associated data carriers.
- (5) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

Attachments

Attachment 1

Technical and organizational measures for data processing security

The following describes which technical and organizational measures are defined to ensure data protection and data security. The aim is to ensure in particular the confidentiality, integrity and availability of the information processed in the company. The structure is based on the internationally recognized standard DIN ISO/IEC 27002.

01. Guideline

The data protection guideline of WiredMinds GmbH contains the guiding statements of the management regarding the handling of personal data in the company. All employees, freelancers and supporting companies are obliged to observe these central regulations. The achieved IT security level of the organizational units, processes and systems is monitored by a combination of periodic audits and continuous controls.

Monitoring of ongoing operations is carried out in coordination with the security officer. A review of the security policy is conducted at least annually, unless an essential change requires it earlier.

This ensures the ongoing adequacy, suitability and effectiveness of the policy. The Safety Officer is the person responsible for the safety policy and has the responsibility to develop, revise, and review it.

02. Information security organization

The managers of WiredMinds GmbH are responsible for the full implementation of the IT security principles in their organizational unit and for fulfilling the IT security tasks assigned to them.

Information security roles and responsibilities are defined in the IT security organization. Conflicting roles and responsibilities are segregated to reduce the potential for unauthorized or unintended modification or misuse of our company's assets.

We have a process in place to determine when and by whom relevant authorities are notified and identified data privacy and information security incidents are reported in a timely manner. We also maintain ongoing contact with special interest groups to keep abreast of changes and improvements in the area of data privacy and information security.

In our projects, data privacy and data security is part of all phases of our project methodology. Through our respective policies and processes on teleworking and the use of mobile devices, we ensure data privacy and data security in these areas as well.

Attachment 1

Technical and organizational measures for data processing security

03. Personnel security

We have carefully selected our employees and reviewed their suitability for their roles in the company. We have defined their responsibilities in job descriptions and regularly check whether the employees comply with them. Before starting their employment, all employees sign a confidentiality and data protection agreement which remains in force after the end of their employment. Employees are trained in data privacy and data security, and in particular training courses are refreshed when they change functions. They are therefore aware of their responsibilities in this regard.

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

04. Management of values

We inventory and maintain all assets (such as equipment, notebooks, smartphones) and information related to personal data.

We have designated responsible parties to protect these assets, who are responsible for the lifecycle of an asset.

Documented rules have been established for the permissible use of our assets. The return of these assets is documented.

Our information and data are classified and labeled based on legal requirements, their value, criticality, and sensitivity to unauthorized disclosure or modification.

In accordance with this classification scheme, we have developed and implemented documented procedures for handling our assets. We do not usually transfer data on removable media, but only in encrypted form via verified communication channels. In exceptional cases, we can only deviate from this practice if instructed to do so in writing by the client.

We dispose of data carriers that are no longer required securely, using a documented procedure and obligated certified service providers.

Attachment 1

Technical and organizational measures for data processing security

05. Access control

We have regulated and documented measures in place to ensure that authorized persons only have access to personal data for which they are authorized to view and process.

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

It is ensured that only authorized users have access to systems and services and that unauthorized access is prevented; in particular, there is a formal process for registering users that enables the assignment of access rights. We grant our administrative rights in a restricted and controlled manner.

We have a documented and regulated process for handling passwords.

Actual and target status of user access rights are regularly compared. If necessary, these are withdrawn or adjusted.

We restrict access to our data as needed and control access to our systems and applications through a secure login process. We employ a system for using strong and secure passwords.

The use of utilities that may be capable of circumventing system and application protections is restricted and closely monitored.

06 Cryptography

The appropriate and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information is ensured. To this end, we have implemented a policy on the use of cryptography within the company, including the management of cryptographic keys, which is appropriate to the need for protection.

Attachment 1

Technical and organizational measures for data processing security

07. Physical and environmental security

We have documented and regulated measures in place to prevent unauthorized persons from gaining access to data processing equipment used to process or use personal data. These include, but are not limited to:

- The business premises are located on the 3rd floor of an office building and are used exclusively
- The central entrance is monitored
- Doors to secure areas are always closed
- Visitors or external service providers are admitted individually
- Fire protection is provided by our hosting partner
- There are security areas 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 failures and malfunctions
- The security of cabling is observed
- Maintenance of systems is planned and implemented
- Removal and changes to systems and information are regulated
- The security of off-premises systems is observed
- Disposal or reuse of equipment is regulated
- Unattended user devices are protected via an automatic screensaver and automatic hard drive encryption
- Clean desk and screen lock policies are implemented

Attachment 1

Technical and organizational measures for data processing security

08. Operational security

We have regulated and documented measures in place to ensure the proper and secure operation of information and data processing facilities. These include, among other things, control in the event of a change to the information-processing facilities, as well as control and regular measurement of our capacities and resources to ensure the availability of the required system performance. For example, the following values, among others, are continuously monitored on an up-to-date basis:

- Hard disk status and available memory
- Raid status
- Services and status of all virtual machines
- Failed login attempts
- Memory usage of the storages and main memory
- Ethernet utilization
- Number of RDP sessions of the individual terminal servers
- Throughput and utilization of the firewall
- Checking the accessibility of all servers is possible via monitoring
- Accessibility and throughput of the switches

A protected procedure for data backup has been implemented by us and is documented.

Standard maintenance windows are defined. Additional necessary windows are announced at least 10 days in advance.

In our company, it is essential to separate development, test and operating environments, so we pay special attention to this.

Measures for detection, prevention and recovery to protect against malware have been taken and are regularly updated.

We have centrally monitored and protected event logging and have privacy measures in place in the event that sensitive personal data is stored. All logging equipment and logging information, including administrators and operator logs are protected from tampering and unauthorized access.

Our clocks are synchronized centrally with a single reference time source.

We have a centralized procedure for the controlled installation of software on systems in our company.

Attachment 1

Technical and organizational measures for data processing security

There is a list of our technical assets and regulated, documented handling in the event of a technical vulnerability, which includes our patch management with defined responsibilities.

We have centrally implemented regulations for restrictions on software installations.

In the event of an audit review of our information systems, we have defined measures to minimize disruptions to business processes as far as possible.

09. communications security

The security of our personal data and information stored in networks and network services is imperative. Therefore, we have implemented documented measures that manage, control and secure our networks.

Information services, users and information systems are kept separate as needed.

We have policies and procedures in place for information and data transfer, as well as information transfer agreements with external entities (e.g., CRM vendors).

Our electronic messaging is appropriately protected. For example, among other things, we have measures in place to protect messages from unauthorized access, alteration, or denial of service that comply with the classification scheme adopted by the organization (protection class 1_E2).

To protect our data, we enter into confidentiality or non-disclosure agreements as needed, which we review regularly.

It is ensured that data and information security is an integral part throughout the lifecycle of our systems. This also includes the requirements for and securing of information systems that provide services via public networks. Transaction protection for application services is performed on an as-needed basis. In addition, we have established a system change management process to ensure the integrity of the system, applications, and products from the early design phases through any subsequent maintenance.

When changes are made to operating platforms, business-critical applications are reviewed and tested to ensure there is no negative impact on organizational security and customer applications. We have a managed process for analyzing, developing, and maintaining secure IT systems.

Acceptance testing programs and associated criteria are established for new information systems, upgrades, and new releases. Our test data is carefully selected, protected and controlled.

Attachment 1

Technical and organizational measures for data processing security

10. Acquisition, development and maintenance of systems

Ensuring that data and information security is an integral part throughout the lifecycle of our systems. This also includes the requirements for and securing of information systems that provide services via public networks. Transaction protection for application services is performed on an as-needed basis. In addition, we have established a system change management process to ensure the integrity of the system, applications, and products from the early design phases through any subsequent maintenance.

When changes are made to operating platforms, business-critical applications are reviewed and tested to ensure there is no negative impact on organizational security and customer applications. We have a managed process for analyzing, developing, and maintaining secure IT systems.

Acceptance testing programs and associated criteria are established for new information systems, upgrades, and new releases. Our test data is carefully selected protected and controlled.

11. supplier relations

We carefully select our suppliers in advance and review their suitability with regard to maintaining data and information security protection.

Documented agreements ensure the protection and confidentiality of our assets and data. Suppliers are required to take technical and organizational measures to ensure this.

There is a regulated and user-defined access authorization to the values and data that are absolutely necessary for the respective supplier.

Suppliers may only engage additional suppliers with our consent in order to ensure a secure supply chain.

We regularly conduct a review of our suppliers' data protection and data security measures to maintain the agreed level. Assigned authorizations are also subject to continuous documented monitoring.

After termination of the supplier relationship, they are obliged to destroy the data and assets received from us. In addition, the maintenance of confidentiality applies indefinitely.

Attachment 1

Technical and organizational measures for data processing security

12. Information security and data privacy incident handling

Our company has a regulated, documented process for handling information security and data privacy incidents to ensure a consistent and effective approach in this regard. Employees are required to report all data privacy and security incidents immediately and receive regular training in this regard. We have installed a reporting system that forwards events to an intervention team to ensure a rapid response. All events are documented, classified and evaluated. The implemented intervention team has precise guidelines on how to respond to an event.

Together with the management, improvement measures resulting from the findings and the collected evidence of an event are discussed and implemented on a regular basis.

13. Information security aspects of business continuity management

As part of information security, the intended availability of systems is specifically assessed and documented. From the requirements, we derive the technical and organizational specifications, such as redundant systems / connections or corresponding planning, and implement them in a consistent and controlled manner.

An overarching emergency plan forms the framework with regard to the corresponding instructions for action for selected documented emergency scenarios.

Continuously updated exercise plans for testing the measures implemented and documentation of the execution of corresponding tests round off the emergency management. All servers and storage systems are leased from a selected data center. Based on the contractual agreements, there is a permanent claim to availability against the service provider.

14. Compliance

We have identified, documented, and keep up-to-date all relevant legal, regulatory, self-imposed, or contractual requirements, as well as our company's procedures for complying with these requirements.

Appropriate procedures have also been implemented to ensure compliance with legal, regulatory, and contractual requirements relating to intellectual property rights and the use of proprietary software products.

In accordance with legal, regulatory, contractual and business requirements, we protect records and personal data as needed. Annual activity reports by the data protection officer document the measures taken.

We observe the regulations on cryptographic measures for this purpose.

To ensure the protection of our information and data, we regularly conduct independent audits of our information security and data privacy levels, our security and data privacy policies, and our compliance with technical requirements.

Attachment 2

The data protection officer appointed for the Contractor is:

Data protection officer of WiredMinds GmbH
c/o activeMind
Potsdamer Str. 3
80802 Munich
Tel. 089-418560170

Phone: +49 (0)89 91 92 94 - 900
www.activemind.de

E-Mail: datenschutzbeauftragter@wiredminds.de

Directory of procedures:

Activemind AG maintains a directory of procedures for WiredMinds GmbH that complies with legal requirements. All WiredMinds employees are contractually bound to data secrecy via their employment contract. WiredMinds employees are demonstrably trained and are familiar with the topics of data security and data protection.

The data protection officer appointed for the client

1. Data protection officer

First name Last name or function designation

Phone

E-Mail

Attachment 3

The following persons are authorized to issue instructions on the part of the Customer:

1. Authorized to issue directives

2. Authorized to issue directives (optional)

Name od function designation

Name od function designation

Phone

Phone

E-Mail

E-Mail

The following persons are authorized to receive instructions from the Contractor:

Nicole Widmann

Datenschutzkoordinator

E-Mail: nicole.widmann@wiredminds.de

E-Mail: datenschutz@wiredminds.de

Phone: 0711 – 585 331 310

Phone: 0711 – 585 331 375

Attachment 4

The following subcontractors are currently being used to perform the contract:

Hetzner Online AG

Industriestr. 25

91710 Gunzenhausen

Germany

Notice:

Technical service provider; sourcing of root servers.

There is NO possibility of the service provider to access data processed on behalf.