Wiredash Data Processing Agreement (DPA)

Last updated: November 4th, 2020

1. Definitions

Controller stands for the natural or legal person, public authority, agency or other body which, alone or jointly with others, defines the purposes and means of the Processing of Personal Data.

Processor stands for a natural or legal person, public authority, agency or other body which handles Personal Data on behalf of the Controller.

Personal Data stands for any information relating to an identified or identifiable individual where such information is contained within Customer Data and is safeguarded similarly as personal data or personally identifiable information under applicable Data Protection Law.

Personal Data Breach stands for a breach of security leading to the unintentional or illicit unauthorized disclosure of, or access to, Personal Data submitted, stored or otherwise processed.

Processing stands for any operation or set of operations which is performed on Personal Data, including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

Data Subject stands for the individual to whom Personal Data relates.

Instruction stands for the written, documented instruction, issued by Controller to Processor, and directing the same to conduct a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

2. Data Processing

1. The Processor shall handle Personal Data for the Purpose as described in the Wiredash Privacy Policy.

- Before or at the time of collecting personal information, the processor detects the objectives for which information is being collected.
- The processor will collect and use personal information solely with the aim of fulfilling compatible purposes, unless the Processor obtains the approval of the controller or as required by law.
- The processor can collect personal information by legal and fair means and, where appropriate, with the knowledge or approval of the Controller.
- Personal data should be relevant to the objectives for which it is to be used, and, to the extent essential for those purposes, should be accurate, complete, and up-to-date.
- The processor shall protect personal information by adequate security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.
- The Processor will only retain personal information as long as required for the fulfillment of those purposes.
- The Processor may only process the Personal Data on documented orders from the Controller, including with regard to transfers to third countries or international organizations, unless required to do so by Union or member state law to which the Processor is subject (in such a case the Processor shall inform the Controller of that legal requirement before processing, unless that law forbids such information on important grounds of public interest).

2. The data is only processed and hosted within a member of the European Union.

- Core infrastructure (Databases, Messaging Servers, APIs) is hosted in Belgium.
- The Processor's server backups are hosted both in the European Union. Those backups are encoded and abundant to prevent any data loss.
- The Processor's content delivery network includes servers outside the European Union. These servers are used as network relays to get endpoints closer from the Data Subject. Those network relays are not saving any customer data and European Data Subjects are in general connected to a server hosted within a member of the European Union.

3. Depending on how the Controller uses the service, the issue of Processing of personal data may include the following types/categories of data:

- IP address
- Email address (if provided by end-user, thus involving a consent)

- In-app screenshots (if provided by end-user, thus involving a consent)
- Message exchanges
- Activity date and time
- Data obtained from public information on Google (Avatar, Name, Twitter/Facebook handle)
- Device type (operating system, device info and browser)
- Preferred language

4. The categories of Data Subjects whose Personal Data are Processed are as follows:

- Wiredash console users (ie. Wiredash project owners)
- Wiredash CRM contacts (ie. the end-users of Wiredash users = users who give feedback through the Wiredash SDK)

3. Technical and organizational provisions

1. The Processor will, considering the nature of the Processing and to the extent that this is reasonably possible, assist the Controller in ensuring compliance with the obligations pursuant to the GDPR to take appropriate technical and organizational measures to guarantee a level of security suitable to the risk. These measures will assure a reasonable level of security, respecting the state-of-the-art and the costs of implementation, with regard to the risks which naturally result from Personal Data Processing and the nature of the data to be protected. The Processor will in any case take measures to safeguard Personal Data against accidental or illicit forgery, unauthorized distribution or access, or any other form of illegal Processing.

- All the features are designed around security and reliability
- Computers and servers running Wiredash development tools are secured and up to date
- All our servers and services are running latest security updates and patched immediacy when a vulnerability is published
- Abusing IPs get automatically banned or rate limited (prevents brute-force attacks on accounts
- We use strong encryption techniques on all public network channels (user messages, user data)
- Two-factor authentication on all third-party services Wiredash uses
- Our SSH keys are all password-protected
- Wiredash employees, agents, and providers are trained in data-security practices

2. The Processor can’t be held responsible when The Controller is using the software or processing data without respecting the technical guidelines or documentation provided by the Processor.

3. The Processor guarantees that its personnel and contractors are instructed about the confidential nature of the Personal Data, have received reasonable training on their responsibilities and underlie obligations of confidentiality.

4. The Controller can contribute or demand audits and inspections but may not carry out an audit more than once per calendar year. The audit shall be performed by an independent third-party company which is neither a competitor of the Processor nor related. The Controller shall repay the Processor for any cost or expenses resulting from the audit.

4. Data Breaches

1. In case the Processor becomes aware of any incident that may have an effect on the protection of Personal Data, he i) will notify the Controller without undue delay, and ii) will take all suitable measures to prevent or limit (further) violation of the GDPR.
2. The Processor will, to a reasonable extent, provide all appropriate cooperation requested by the Controller in order for the Controller to comply with his legal obligations relating to the identified incident.
3. The Processor will, to a reasonable extent, assist the Controller with the Controller's notification obligation concerning the Personal Data to the Data Protection Authority and/or the data subject, as meant in Section 33(3) and 34(1) GDPR. The Processor is never held to report a personal data breach with the Data Protection Authority and/or the data subject.
4. The Processor will not be responsible and/or liable for the (punctual and correct) notification obligation to the relevant supervisor and/or data subjects, as meant in Section 33 and 34 GDPR.

5. Sub-Processors

1. Sub-processing in the meaning of this agreement does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measurements to guarantee the confidentiality, availability, integrity and resilience of the hardware and software of the data Processing equipment.
2. The Processor is authorized to outsource the implementation of the Processing of the Controller's instructions to Sub-processors, both wholly or in part. The Processor will inform the Controller of any planned changes regarding the addition or replacement of other processors.
3. The Processor instructs and obliges each Sub-processors to contractually comply with the confidentiality obligations, notification obligations and security measurements concerning the Processing of Personal Data, which obligations and measurements must at least comply with the provisions of this Processor's Agreement.
4. The Controller reserves the right to object to any Sub-processor, provided that, in his opinion, the Sub-processor data does not provide sufficient guarantees to execute adequate technical and organizational data protection measurements.
5. Where the controller, with regard to the obligations under the GDPR, is obliged to provide information to a Data Subject about the Processing of his or her Personal Data, the Processor shall assist the Controller in making this information available. The Processor shall quickest possible and in the most detailed manner

conceivable refer the requests of complaints of the Data Subject to the Controller and shall assist the Controller with any request from a Data Subject concerning his or her rights under Applicable Legislation, and in particular - but not restricted to - his or her right of access, rectification, correction, objection, restriction of processing, the right to be forgotten and the right of data portability. The Processor shall correct, erase or process the data in any other way if the Controller instructs him to enable the latter to comply with the request of the Data Subject.

6. The Controller agrees to the commissioning of the following sub-processors on the condition of a contractual agreement in accordance with the applicable data protection laws:

Sub-Processor	**Country**	**Service**
Cloudflare, Inc.	USA	CDN Provider
Google, LLC	USA	Hosting Provider
Paddle.com Market Limited	England	Payment Provider
Twilio, Inc.	USA	Email Notifications

6. Duration

1. This agreement shall begin on the Commencement Date and shall continue in full force and effect until the termination of the Purpose.
2. The Controller will correctly inform the Processor about the statutory retention periods that apply to the Processing of Personal Data by the Processor.

7. Rectification, restitution and erasure of data

1. The processor may not on its own authority correct, erase or restrict the Processing of Personal Data that is being processed on behalf of the Controller (unless if this is required by law), but shall only do so on documented instructions from the Controller and in accordance to data retention rules associated to the Controller´s subscription plan. Upon expiry of the DPA, the Processor shall, at the choice of the Controller, return all the Personal Data transferred and the equivalent copies to the Controller, or shall delete and/or anonymize all the Personal Data in an irreversible manner and prove to the Controller that he has done so, unless the Applicable Legislation imposed upon the Processor prevents him from returning or destroying all or part of the Personal Data Processed.
2. If a Data Subject should apply directly to the Processor with the request of rectification, erasure, or restriction of his Personal Data, the Processor must forward this request to the Controller without undue delay.