Data Processing Agreement

Version: 1.0.1
Last Updated: August 10, 2024

Purpose of the Agreement

In connection with the contractual relationship between Wiredash GmbH, Turmstraße 28, 40789 Monheim, Germany (hereinafter referred to as the "Processor") and the customer (hereinafter referred to as the "Customer," and together with the Processor, the "Parties") for the use of the Processor's software by the Customer (the "Contract"), the Processor may handle personal data as defined by Article 4(1) of the General Data Protection Regulation ("GDPR"), which includes any information pertaining to an identified or identifiable individual (for example, the names, addresses, or phone numbers of the Customer's clients). In this context, the Customer acts as the data controller under data protection laws (referred to as "Customer Data"). This agreement (the "Agreement") outlines the data protection duties and rights of the Parties in relation to the Processor's handling of Customer Data for the purpose of delivering the services under the Contract.

Scope of Processing

1. The Processor will handle Customer Data on behalf of and according to the instructions of the Customer in accordance with Article 28 of the GDPR. The Customer retains the role of data controller as defined by Article 28 of the GDPR.

2. The Processor's processing of Customer Data will be carried out as described in Annex A of this Agreement, which specifies the method, extent, and purpose of the processing, as well as the types of personal data and categories of individuals involved. The duration of the processing is aligned with the term of the Contract.

3. The Processor has the right to anonymize or aggregate Customer Data in such a way that it can no longer be linked to individual data subjects, and to use this anonymized or aggregated data for purposes such as product development, optimization, and service delivery as specified in the Contract. The Parties agree that once Customer Data has been anonymized or aggregated in this way, it will no longer be considered Customer Data under this Agreement.

4. The Processor may also process and utilize Customer Data for its own purposes as a data controller, where permitted by applicable data protection laws. This Agreement does not govern such processing.
5. The Processor will generally process Customer Data within the European Union or another member state of the European Economic Area (EEA). However, the Processor may process Customer Data outside the EEA if the Processor informs the Customer in advance (for example, in the privacy policy), and if the requirements of Articles 44 to 48 of the GDPR are met or if an exception under Article 49 of the GDPR applies.

Customer’s Right to Issue Instructions

1. The Processor will process Customer Data in line with the Customer’s instructions unless the Processor is legally obligated to do otherwise. In such cases, the Processor will notify the Customer of the legal obligation prior to processing unless prohibited by law on significant public interest grounds.

2. The Customer’s instructions are generally documented and finalized in this Agreement. Any individual instructions that differ from this Agreement or impose additional requirements must be mutually agreed upon by the Processor.

3. The Processor will ensure that Customer Data is processed according to the Customer’s instructions. If the Processor believes that an instruction from the Customer violates this Agreement or applicable data protection laws, the Processor is entitled, after notifying the Customer, to suspend the execution of the instruction until the Customer confirms it. The Parties agree that the Customer is solely responsible for ensuring that Customer Data is processed according to the instructions provided.

Customer’s Legal Responsibility

1. The Customer is solely responsible for ensuring the lawful processing of Customer Data and for protecting the rights of data subjects in relation to the Processor. If any third parties bring claims against the Processor due to the processing of Customer Data as per this Agreement, the Customer will indemnify the Processor against all such claims upon first request.

2. The Customer is responsible for providing the Processor with Customer Data in a timely manner to enable service delivery as per the Contract and for ensuring the accuracy and quality of the Customer Data. The Customer will promptly inform the Processor if any errors or irregularities related to data protection provisions or Customer instructions are identified during the review of the Processor's results.

3. Upon request, the Customer will provide the Processor with the information required under Article 30(2) of the GDPR, as far as it is not already available to the Processor.

4. If the Processor is required to provide information to a governmental authority or third party regarding the processing of Customer Data or to cooperate with these authorities in any way, the Customer is obligated to assist the Processor promptly in providing such information and fulfilling other necessary cooperation requirements.

Personnel and System Requirements

The Processor will ensure that all personnel involved in processing Customer Data are committed to maintaining confidentiality regarding the processing of Customer Data.

Security Measures for Data Processing

1. The Processor will implement necessary and appropriate technical and organizational measures as per Article 32 of the GDPR, considering the state of the art, the implementation costs, the nature, scope, context, and purposes of processing, as well as the varying risks to the rights and freedoms of data subjects, to ensure a level of security appropriate to the risk. These measures are detailed in Annex B.

2. The Processor reserves the right to adjust technical and organizational measures during the term of this Agreement, provided they continue to meet statutory requirements.

Use of Subprocessors

1. The Customer grants the Processor general authorization to engage subprocessors to handle Customer Data. Subprocessors engaged at the time of this Agreement's signing are listed in Annex C. Authorization is generally not required for contracts with service providers responsible for inspecting or maintaining data processing systems or for additional services, even if access to Customer Data is possible, provided that the Processor takes appropriate measures to safeguard the confidentiality of Customer Data. Subprocessor notifications will be provided at least 14 days before any changes, allowing the Customer to raise objections. The Customer may only object for significant reasons, which must be clearly stated to the Processor. If the Customer does not object within 14 days of receiving the notification, the Customer's right to object will lapse. If the Customer does object, the Processor may terminate the Contract and this Agreement with three months' notice.

2. The Processor's agreement with any subprocessor must ensure that the subprocessor is bound by the same obligations that apply to the Processor under this Agreement. The Parties agree that this requirement is fulfilled if the contract provides a level of protection equivalent to this Agreement.

3. In compliance with Section 2.5 of this Agreement, these provisions also apply if a subprocessor is located in a third country. The Customer hereby authorizes the Processor to enter into an agreement with a subprocessor on the Customer's behalf based on the standard contractual clauses for data transfers to processors in third countries, as adopted by the European Commission on June 4, 2021. The Customer agrees to cooperate as necessary to meet the requirements of Article 49 of the GDPR.

Rights of Data Subjects

1. The Processor will reasonably assist the Customer by implementing technical and organizational measures to help the Customer respond to requests from data subjects exercising their rights.

2. If a data subject submits a request to the Processor directly, the Processor will promptly forward the request to the Customer.

3. The Processor will provide the Customer with information on the stored Customer Data, the recipients of the data, and the purpose of the data storage, as far as the Customer does not already have this information and is unable to obtain it independently.

4. The Processor will assist the Customer in correcting, deleting, or restricting the processing of Customer Data, or will carry out these actions itself at the Customer's instruction, to the extent that the Customer cannot do so independently. The Processor will be compensated for any substantiated costs incurred in this regard.

5. If a data subject has the right to data portability under Article 20 of the GDPR regarding Customer Data, the Processor will assist the Customer, as needed, in providing the data in a structured, commonly used, and machine-readable format, provided the Customer is unable to obtain the data independently. The Processor will be compensated for any substantiated costs incurred in this regard.

Notification of Data Breaches

1. Should the Customer be legally obligated to inform authorities about a security breach involving Customer Data (specifically under Articles 33 and 34 of the GDPR), the Processor must promptly notify the Customer of any such incidents within the Processor's responsibility. The Processor will assist the Customer in meeting these notification requirements as needed, with reasonable efforts. The Processor is entitled to reimbursement for any verified costs incurred during this process.

2. Additionally, the Processor will, upon request and as reasonably necessary, support the Customer in conducting data protection impact assessments and subsequent consultations with regulatory authorities, as required under Articles 35 and 36 of the GDPR. The Customer will compensate the Processor for any associated and substantiated expenses.

Deletion and Return of Customer Data

1. Following the conclusion of the Contract or upon the Customer's request, the Processor will delete or return all Customer Data, including any copies thereof,

unless the Processor is legally required to retain the data. The method of deletion will align with industry standards to ensure that the data cannot be reconstructed.

2. Even after the termination of the Agreement, the Processor may keep records that demonstrate compliant and accurate handling of the Customer Data.

Audits and Inspections

1. At the Customer's request, the Processor will provide all necessary and available information to demonstrate adherence to the obligations under this Agreement.

2. The Customer has the right to verify the Processor's compliance with this Agreement, including its implementation of technical and organizational measures, through audits (including inspections).

3. For inspections under Section 11.2, the Customer may visit the Processor's premises where Customer Data is processed during normal business hours (Monday to Friday, 10 am to 6 pm) after giving appropriate advance notice as outlined in Section 11.5. These inspections will be conducted at the Customer's expense, without disrupting the Processor's operations, and with strict confidentiality concerning the Processor's business and trade secrets.

4. The Processor may, at its discretion and in consideration of the Customer's legal obligations, withhold information that is sensitive to the Processor's business or would breach legal or contractual provisions. The Customer is not permitted to access information regarding the Processor's other clients, cost structures, quality assurance reports, contract management details, or any other confidential information unrelated to the audit's purpose.

5. The Customer must notify the Processor well in advance (typically at least two weeks) of any details related to the audit. The Customer is entitled to conduct only one audit per calendar year.

6. If the Customer engages a third party to carry out the audit, the Customer must ensure that the third party is bound by the same confidentiality and secrecy obligations that apply to the Customer under this Section. The Customer must also obligate the third party to maintain confidentiality via a written agreement unless the third party is already subject to professional secrecy obligations. Upon the Processor's request, the Customer must immediately provide the Processor

with the third party's confidentiality agreements. The Customer is not permitted to engage any of the Processor's competitors to conduct the audit.

7. As an alternative, the Processor may provide proof of compliance with its obligations under this Agreement by submitting a current report or certification from an independent authority (such as an auditor, internal audit department, data protection officer, IT security department, or quality auditor) or an appropriate IT security or data protection certification ("Audit Report"). This Audit Report must enable the Customer to verify the Processor's compliance with the contractual obligations adequately.

Term and Termination

The length and termination of this Agreement are subject to the terms and conditions of the Contract. The termination of the Contract will automatically result in the termination of this Agreement. The Agreement cannot be terminated separately.

Liability

1. The Processor's liability under this Agreement is governed by the limitations and disclaimers set forth in the Contract. If third parties bring claims against the Processor due to the Customer's failure to meet its obligations under this Agreement or any of its responsibilities as the data controller, the Customer agrees to indemnify and hold the Processor harmless from these claims upon the first request.

2. The Customer also agrees to indemnify the Processor for any fines imposed on the Processor that correspond to the Customer's share of responsibility for the violation leading to the fine.

Final Provisions

1. If any part of this Agreement is found to be invalid or becomes invalid, or if there is a gap in the Agreement, the rest of the Agreement will remain unaffected. The Parties agree to replace the invalid provision with a valid one that closely reflects the original purpose and complies with Article 28 of the GDPR.

2. In the event of any conflict between this Agreement and other agreements between the Parties, particularly the Contract, the terms of this Agreement will take precedence.

3. This Agreement is governed by the laws of Germany, and any disputes arising from or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts in Düsseldorf, Germany.

Annex A

Further Information on the Processing of Customer Data

Purpose of the processing	The performance of the Services, specifically the delivery of tooling services for developing and operating multi-platform applications.
Categories of personal data stored or processed through the Services	○ Account data (e.g. first name, last name, email, profile picture) ○ Contact data (e.g. first name, last name, email) ○ Usage data ○ Any data provided by the Customer through the SDK ○ User-generated data
Categories of data subjects to whom the personal data mentioned above relates	○ Users of the Wiredash software (Wiredash Console) ○ Users who engage with the Wiredash SDK via the Customer's app ○ Users of the Customer's app that incorporates the Wiredash SDK
Nature of the processing	Storage, deletion, rectification, analysis, transfer, aggregation
Frequency of the transfer	Continuous
Retention period	The duration of the Agreement, unless earlier deletion is requested by the Customer in accordance with the functionality of the Services.
Subprocessors	As set out out in Annex C

Annex B

Technical and Organizational Measures

The processor implements a combination of policies, procedures, guidelines, and technical and physical controls to protect the personal data it processes from accidental loss, unauthorized access, disclosure, or destruction.

Governance and Policies

The processor assigns personnel who are specifically responsible for determining, reviewing, and implementing security policies and measures. These individuals ensure that all security protocols are effectively managed and enforced throughout the organization.

To maintain the effectiveness of its security protocols, the processor conducts regular reviews of its security measures and policies. These reviews are carried out to ensure that the protocols continue to be suitable and effective for the protection of the data being processed.

In addition, the processor establishes and adheres to secure configurations for its systems and software. This practice ensures that security measures are integrated from the very beginning of project initiation and are consistently applied during the development of new IT systems.

Breach Response

The processor maintains internal monitoring systems that can alert its operational teams to any service outages, sometimes even before outage thresholds are reached.

The processor has developed a breach response plan to address data breach events, which is regularly tested and updated.

Access Controls

The processor limits access to personal data by implementing appropriate access controls, including:

1. Access to infrastructure and internal resources is managed based on the Principle of Least Privilege: individuals are granted only the privileges necessary to perform their business duties, and these privileges are revoked when no longer needed.

2. Access management is centralized through identity providers, and wherever feasible, internal services delegate both authentication and authorization to these providers, ensuring timely off-boarding and privilege revocation.

3. The processor's infrastructure changes require approval from at least one additional authorized person, with designated persons based on the system's relevance to their business roles.

4. User authentication for the processor's internal resources is protected by a strong password policy and mandatory 2FA, which excludes SMS-based 2FA.

5. The processor never knowingly stores plaintext passwords; if necessary, it stores hashed, salted authentication materials as appropriate for the use case.

6. The processor's devices used for accessing internal resources enforce strong security measures, including strong passwords, antivirus software, and full-disk encryption.

7. Audit trails of user actions within the processor's infrastructure are retained, including logs of all interactions with its internal services and Customer projects.

8. Traffic flow logs are retained to enable retroactive analysis of all connections to our infrastructure if needed.

9. Only pre-approved and secure communication methods with the processor's services are exposed by its firewalls.

10. All communication, including transmission of credentials, is conducted over connections protected by TLS configured with modern cipher suites.

Segmentation

Databases with customer data and internal services are deployed in separate networks with firewall rules ensuring that only expected traffic between the two is allowed. Additionally, logs are retained of metadata about the traffic flowing across the two.

Logs and metrics used for observability and debugging are automatically extracted and sent to systems that are segregated from customer projects containing the user's data.

Encryption

Stored data is encrypted where appropriate, including any backup copies.

All data is encrypted at rest using the industry-standard AES-256 algorithm. Regularly scheduled backups are also encrypted at rest using AES-256.

All network communication is conducted over encrypted links protected by modern security standards (TLS 1.2, modern cipher suites) to ensure the confidentiality and integrity of the data.

Availability and Backup

The processor takes daily backups of Customer projects by default. Additional backups can be scheduled based on Customer requirements and service agreements.

All backups are encrypted in transit and at rest.

Testing

Wiredash uses reasonable and appropriate security and compliance monitoring systems across its infrastructure to detect any violations of its security policies.

Annex C

Further Processors

Name of the processor	**Description of processing**
ClickHouse Inc. 650 Castro St, Ste. 120 Unit 92426, Mountain View, CA 94041, United States	Managed database platform
GitHub Inc. 88 Colin P Kelly Jr St, San Francisco, CA 94107, United States	Social sign in provider
Google LLC 1600 Amphitheatre Parkway,	Secure cloud service platform

Mountain View, CA 94043, United States	
MongoDB Ltd. Building Two Number One Ballsbridge, Ballsbridge, Dublin 4, Ireland	Managed database platform
Paddle.com Market Ltd. Judd House 18-29 Mora Street, London, EC1V 8BT, United Kingdom	Payment platform for processing subscriptions
Sendgrid Twilio Germany GmbH Rosenheimer Str. 143C, 8167 Munich, Germany	Provider for transactional email services
Sentry / Functional Software, Inc. 45 Fremont Street, 8th Floor, San Francisco, CA 94105, United States	Monitoring and securing of SaaS applications
Vercel Inc. 440 N Barranca Ave #4133, Covina, CA 91723, United States	Hosting provider