Data Processing Agreement

CONTRACT DETAILS

SUPPLIER

Company Name and Company Number: Doozy Live Ltd (with company number: 12623619)
Address: 128 City Road, London, EC1V2NX
Email: privacy@doozy.live

CUSTOMER

Company Name:
Address:
Email:

Each of the parties shall be referred to as a **Party** or together, the **Parties**.

PROCESSING DETAILS

Purpose	For the purpose of the Supplier providing Doozy (An employee experience platform, built for Slack and the Web) to the Customer.
Scope and nature of the processing	Receiving data, including collection, accessing, retrieval, recording, and data entry. Holding data, including storage, organization, and structuring Using data, including analysis, consultation, testing, automated decision making, and profiling Updating data, including correcting, adaptation, alteration, alignment, and combination Protecting data, including restricting, encrypting, and security testing Sharing data, including disclosure, dissemination, allowing access, or otherwise making available Returning data to the data exporter or data subject Erasing data, including destruction and deletion

Categories of data subject	Employees
Categories of personal data	Name Contact information such as email, phone number, or address Employment information such as employee ID, Birthday, Start Date, End Date, Manager, Team, Professional or biographic information such as resume or CV User activity and analysis such as device information or IP address
Duration of Processing	For the duration that the Supplier provides Doozy to the Customer which is for as long as it is necessary for the Supplier to process Customer Personal Data to fulfil the Purpose.
Data Protection Officer(s)	The Supplier's data protection officer is Milo Hill

---

BACKGROUND

A. The Supplier is providing services to the Customer where the Supplier is required to process Customer Personal Data to fulfil the Purpose (as defined in the Contract Details).

B. This Agreement sets out the terms on which the Supplier will process the Customer Personal Data, in accordance with Data Protection Laws.

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

Agreement: refers to this Data Processing Agreement and includes the Contract Details and any Schedules attached to it.

Customer Personal Data: the personal data processed by the Supplier on behalf of the Customer under this Agreement. This Personal Data is detailed as the 'Scope and nature of processing', the 'Categories of personal data' and the 'Categories of data subjects' in the Contract Details at the front of this Agreement.

Contract Details: refers to the terms agreed between the Parties on the front pages of this Agreement titled "Contract Details".

Data Protection Laws means all applicable data protection and privacy laws, their implementing regulations, regulatory guidance, and secondary legislation, each as updated or replaced from time to time, including, as they may apply: (i) the General Data Protection Regulation ((EU) 2016/679) (the "GDPR") and any applicable national implementing laws; (ii) the UK General Data Protection Regulation ("UK GDPR") and the UK Data Protection Act 2018; (iii) U.S. legislation (e.g., the

California Consumer Privacy Act and the California Privacy Rights Act); and (iv) any other laws that may be applicable.

Data controller, **data processor, data subject**, **personal data, processing** and **appropriate technical and organisational measures** shall have the meanings given to them in the UK GDPR.

Duration of Processing: the length of time the Supplier will process the Customer Personal Data as described in the Contract Details at the front of this Agreement.

DP Regulator: a valid supervisory authority (as defined under the UK GDPR), which in the UK is the Information Commissioner.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Purpose: means the purpose for processing the Customer Personal Data, as detailed in the Contract Details.

Sub-Processor(s): any processor, including any agent, sub-contractor or other third party, engaged by the Supplier (or by any other Sub-Processor) for carrying out any processing activities in respect of the Customer Personal Data.

1.2 A person means an individual, a firm, a company, an unincorporated body or a government entity (whether or not having a separate legal identity from its members or owners) and any of its successors, permitted transferees or permitted assignees.

1.3 Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

1.4 References to statutes, regulations or other legislation or enactments referenced herein shall be deemed to be references to that enactment as amended, supplemented, re-enacted or replaced from time to time.

1.5 The words include, including and similar words or expressions will not limit the meaning of the words that come before them.

1.6 Reference to writing or written includes e-mail but not any other form of electronic communication.

2 DATA PROTECTION ROLES AND RELATIONSHIP

2.1 The Parties acknowledge that the Customer is the data controller of the Customer Personal Data uploaded, stored and/or transmitted by the Customer’s personnel via Doozy and the Supplier is the data processor of the Customer Personal Data.

2.2 Both Parties will comply with all applicable requirements of Data Protection Laws in relation to personal data that is shared or processed under this Agreement. This Agreement does not relieve, remove or replace, a Party's obligations or rights under applicable Data Protection Laws.

3 DATA PROCESSING OBLIGATIONS

3.1 Each Party shall maintain records which indicate how that Party processes personal data under its responsibility. These records will contain at least the minimum information required by the Data Protection Laws and each Party shall make that information available to any DP Regulator on request.

3.2 To the extent that the Supplier processes Customer Personal Data on behalf of the Customer, the Supplier shall:

3.2.1 process that Customer Personal Data only on the documented instructions of the Customer, which shall include processing the Customer Personal Data to the extent necessary for the Purpose, unless the Supplier is otherwise required by applicable laws. The Supplier shall notify the Customer if its instructions infringe Data Protection Laws or other applicable laws;

3.2.2 implement appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, including as appropriate:

a) the pseudonymisation and encryption of Customer Personal Data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

3.2.3 Notwithstanding the obligations in clause 3.2.2, the Supplier shall comply at all times with its security policy, as set out in the attachment to this Agreement (Attachment 1);

3.2.4 maintain the confidentiality of the Customer Personal Data, not disclose the Customer Personal Data to any third party other than as authorised to do so under this Agreement and ensure that any personnel engaged and authorised by the Supplier to process Customer Personal Data have committed themselves to obligations of confidentiality;

3.2.5 assist the Customer in responding to any request from a data subject and in ensuring the Customer's compliance with its obligations under applicable Data Protection Laws. This process shall be provided (at the Customer’s cost) and shall include:

a) recording and referring all requests and communications received from data subjects or any DP Regulator to the Customer which relate to any Customer Personal Data promptly (and in any event within one month of receipt); and
b) not responding to any such requests without the Customer’s express written approval and strictly in accordance with the Customer’s instructions unless and to the extent required by applicable law.

3.2.6 promptly (and in any event within 72 hours):

a) notify the Customer if it (or any of the Sub-Processors or the Supplier personnel) becomes aware of any actual occurrence of any Personal Data Breach in respect of any Customer Personal Data; and
b) provide all information as the Customer reasonably requires to report the circumstances to a DP Regulator and to notify affected data subjects under Data Protection Laws.

3.3 Where the Supplier is relying on applicable laws as the basis for processing Customer Processor Data under clause 3.2.1 above, the Supplier shall use reasonable efforts to notify the Customer of this before performing the processing required by the applicable laws unless those applicable laws prohibit the Supplier from so notifying the Customer.

4 SUB-PROCESSORS

4.1 The Customer hereby provides its prior, general authorisation for the Supplier to appoint Sub-Processors to process the Customer Personal Data, provided that the Supplier:

4.1.1 shall ensure any Sub-Processors will comply with applicable Data Protection Laws, and will comply with terms that are materially similar to those imposed on the Supplier in this clause 4;

4.1.2 shall remain responsible for the acts and omissions of any such Sub-Processor as if they were the acts and omissions of the Supplier; and

4.1.3 shall inform the Customer of any intended changes concerning the addition or replacement of the Sub-Processors; giving the Customer the opportunity to object to such changes. Where the Customer objects to the changes and cannot demonstrate, in the Supplier's reasonable opinion, that the objection is due to an actual or likely breach of applicable Data Protection Law, the Customer shall indemnify the Supplier for any losses, damages, costs (including legal fees) and expenses suffered by the Supplier in accommodating the objection.

A list of the Supplier's subprocessors is available at https://doozy.live/subprocessors

5 INTERNATIONAL TRANSFERS

5.1 The Supplier may transfer Customer Personal Data outside of the United Kingdom and European Economic Area as required to process the Customer Personal Data for the Purpose under this Agreement, provided that the Supplier shall ensure that all such transfers are made in accordance with applicable Data Protection Laws. For these purposes, the Customer shall promptly comply with any reasonable request of the Supplier, including any request to enter into standard data protection clauses to safeguard international transfers, as adopted by the UK Information Commissioner. Supplier and Customer agree to use the Standard Contractual Clauses as the adequacy mechanism supporting the transfer and Processing of Customer Personal Data, as further detailed below.

5.1.1 2021 Standard Contractual Clauses. For transfers of Customer Personal Data out of the EEA that are subject to this Section 5.1, the 2021 Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the 2021 Standard Contractual Clauses will apply as set forth in this Section 5.1.1 “Module Two: Transfer controller to processor” will apply and all other module options will not apply. Under Annex 1 of the 2021 Standard Contractual Clauses, the “data exporter” is Customer and the “data importer” is Supplier and the information required by Annex 1 can be found in the Contract Details. For the purposes of Annex 2 of the Standard Contractual Clauses, the technical and organisational measures implemented by the data importer are those listed in Section 3. Clause 7 will not apply. For clause 9, the Parties choose Option 2 and the Parties agree that the time period for prior notice of Third Party changes will be as set forth in Section 4. For clause 11, the optional language will not apply. For clause 17, the Parties choose Option 1 and the Parties agree that the governing law will be the Republic of Ireland. For clause 18, the Parties agree that the courts of the Republic of Ireland will apply for subsection (b).

5.1.2 UK Standard Contractual Clauses. For transfers of Customer Personal Data out of the United Kingdom that are subject to Section 5.1 of this Addendum, the UK Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the UK Standard Contractual Clauses will apply as set forth in this Section 5.1.2. For Table 1 of the UK Standard Contractual Clauses, (i) the Parties’ details shall be the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Annex 1 of the 2021 Standard Contractual Clauses and (ii) the Key Contacts shall be the contacts set forth in Annex 1 of the 2021 Standard Contractual Clauses. The Approved EU SCCs referenced in Table 2 shall be the 2021 Standard Contractual Clauses as executed by the Parties pursuant to this Addendum. For Table 3,

Annex 1A, 1B, and II shall be set forth in Annex 1 of the 2021 Standard Contractual Clauses. For Table 4, either party may end the UK Standard Contractual Clauses as set out in Section 19 of the UK Standard Contractual Clauses.

6 Each party's signature to this Data Processing Agreement shall be considered a signature to the Standard Contractual Clauses. If required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Standard Contractual Clauses as separate documents. In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail.

6 AUDIT

6.1 The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Customer.

6.2 Such records shall include all information necessary to demonstrate its compliance with this Agreement and the information referred to in Articles 30(1) and 30(2) of the UK GDPR.

6.3 The Supplier shall make copies of such records referred to in this clause 6 available to the Customer promptly on written request by the Customer.

6.4 The Supplier shall (and shall ensure all Sub-Processors shall) promptly on written request by the Customer make available to the Customer (at no cost the Customer) such information as is required to demonstrate the Supplier's with their obligations under this Agreement and the Data Protection Laws, and allow for, permit and contribute to audits, including inspections, by the Customer (or another auditor instructed by the Customer) for this purpose annually (if requested) and in the event of an actual or suspected Personal Data Breach.

6.5 Except in the event of an actual or suspected Personal Data Breach, the Customer shall provide no less than 30 days notice to the Supplier of any audit under this clause 6 and shall use reasonable endeavours to cause minimal disruption to the Supplier's business during any such audit.

7 TERMINATION AND EFFECT OF TERMINATION

7.1 This Agreement shall remain in full effect for the Duration of Processing following which it shall automatically terminate.

7.2 Where the Supplier no longer requires the Customer Personal Data for the Purpose, it shall, at the written direction of the Customer, delete (so far as technically possible) or return Customer Personal Data and any copies to the Customer within 30 days of termination of this Agreement, unless the Supplier is required by any applicable law to continue to process that Customer Personal Data.

7.3 For the purposes of this clause 7, Customer Personal Data shall be considered deleted where it can longer be used further by the Supplier.

8 GENERAL

8.1 Costs

Each Party is responsible for its legal and other costs in relation to the preparation and performance of this Agreement.

8.2 Survival of terms

The Parties intend the following terms to survive termination: clauses 1, 6, 7, and 8 and all clauses required for their interpretation.

8.3 Relationship of the Parties

The Parties are independent businesses and not partners, principal and agent, or employer and employee, or in any other relationship of trust to each other.

8.4 Third party rights

For the purposes of the Contracts (Rights of Third Parties) Act 1999, this Agreement is not intended to and does not give any person who is not a party to it any right to enforce any of its provisions. However, this does not affect any rights or remedy of such a person that exists or is available apart from that Act.

8.5 Assignment and other dealings

No Party may assign, subcontract or encumber any right or obligation under this Agreement, in whole or in part, without the other Party's prior written consent or except as expressly permitted in this Agreement.

8.6 Entire Agreement

This Agreement, and any document referred to in it, contains the whole Agreement between the Parties relating to its subject matter and supersedes any prior Agreements, representations or understandings between them unless expressly referred to in this Agreement. Each Party acknowledges that it has not relied on, and will have no remedy in respect of, any representation (whether innocent or negligent) made but not covered in this Agreement. Nothing in this clause limits or excludes any liability for fraud or fraudulent misrepresentation.

8.7 Variation

No amendment or variation of this Agreement will be valid unless agreed in writing by an authorised signatory of each Party.

8.8 Severability

If any clause in this Agreement (or part of a clause) is or becomes illegal, invalid or unenforceable under applicable law, but would be legal, valid and enforceable if the clause or some part of it was deleted or modified (or the duration of the relevant clause reduced), the relevant clause (or part of it) will apply with such deletion or modification as may be required to make it legal, valid and enforceable, and the Parties will promptly and in good faith seek to negotiate a replacement provision consistent with the original intent of this Agreement as soon as possible.

8.9 Waiver

No delay, act or omission by either Party in exercising any right or remedy will be deemed a waiver of that, or any other, right or remedy.

8.10 Notices

Notices under this Agreement must be in writing and sent to the other Party's address, as set out above in the Contract Details. Letters sent in the United Kingdom will be deemed delivered 3 business days (excluding English Bank Holidays), after sending. Emails will be deemed delivered the same day (or the next business day, if sent on a non-business day or after 5pm on any business day at the recipient's location).

8.11 Counterparts

This Agreement may be signed in any number of counterparts and by the Parties on separate counterparts, each of which when signed and dated will be an original, and such counterparts taken together will constitute one and the same Agreement. This Agreement will not be effective until each Party has signed one counterpart.

8.12 Governing law and jurisdiction

This Agreement is governed by the law of England and Wales. All disputes under this Agreement will be subject to the exclusive jurisdiction of the courts of England and Wales.

By signing below the Parties agree to the terms set out in this data processing agreement, with effect from the date that it is signed by both Parties.

Signed for and on behalf of Doozy Live Ltd by

08 November 2023

Milo Hill
CEO
Doozy Live Ltd

Signed for and on behalf of _____

Name:
Title:
Company:

Attachments

Attachment 1 Security Policy

Security at Doozy

Pseudonymization and encryption of personal data
Customer data is encrypted at rest with 256-bit AES.

Secure tokens for Slack, Merge and Google Calendar are further encrypted with AES-128 and rotated monthly.

Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services
Doozy runs on Google Cloud Infrastructure, which offers a Service Level Agreement (SLA) that guarantees a certain level of uptime and availability for services, including Firestore (with a guaranteed uptime of ≥99.99%) and Storage (with a guaranteed availability of ≥99.9%).

Data is encrypted in transit using HTTPS (≥ TLS 1.2).

We conduct monthly vulnerability scans to ensure systems are configured correctly and are up to date.

Ability to restore the availability of and access to the Customer Personal Data in a timely manner following a physical or technical incident:
Daily, weekly and point-in-time backups are encrypted and stored in multiple regions for redundancy.

Our customers have access to support through Slack Connect, with a standard SLA response time of under 12 hours, usually much quicker!

Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures used to secure Processing:
Monthly scans are conducted to check for network vulnerabilities. Automated testing is run automatically for all code deploys.

User identification and authorization process and protection
Strong security measures are enforced, including password complexity and MFA to ensure access to production systems is secure.

Role-based access control is in place through groups and IAM to ensure access to data is on a strictly need-to-know basis.

Access to production data is time-limited and requires exec approval, and it is fully audited.

Protecting Customer Personal Data during transmission (in transit):
All communications are encrypted in transit over HTTPS.

Protecting Customer Personal Data during storage (at rest):
Customer data is encrypted at rest with 256-bit AES.

Physical security where Customer Personal Data is processed
Customer data is stored securely within the Google data centers, and protected 24/7 by their industry-leading security team.

Security measures include perimeter defense systems, comprehensive camera coverage, biometric authentication, and a 24/7 guard staff. Learn more here.

Events logging
Audit logs are enabled and configured for all production environments using GCP Cloud Audit Logging.

Access to production data requires C-Level approval and is time limited.

Detailed application logs are produced to track user activities, errors, exceptions and security events. On-call engineers are automatically notified of customer and security impacting issues.

Systems configuration, including default configuration:
Infrastructure is running fully serverless in Google Cloud and Vercel, and security patches and updates are automatically applied.

Firebase infrastructure configuration is managed through code and reviewed via pull requests.

Internal IT and IT security governance and management:
Devices are managed through an MDM, and strict policies are in place to ensure that the best security standards are being upheld by staff such as device locking, secure password policies and MFA.

Access to production systems is heavily monitored and access time-limited and audited on a need-to-know basis.

Certification or assurance of processes and products:
Our infrastructure runs on Google Cloud, which maintains a wide range of industry certifications, including ISO 27001, SOC 2, and others, which reflect its commitment to security and compliance. These certifications extend to the infrastructure services used.

All subprocessors handling customer data are SOC2 or ISO 27001 compliant.

The SOC 2 certification process is planned for Q1 2024.

Ensuring data minimization:
Doozy follows a strict data collection and processing policy. We collect and retain only the data necessary for specific, well-defined purposes.

We regularly review and minimize the data we hold, ensuring its relevance and accuracy. Access to this data is tightly controlled, and data subjects' rights, including the right to access and erasure, are respected.

Ensuring data quality
Data is kept up to date through periodic and real-time syncs between external systems such as Merge, Slack, and Google Calendar.

Thorough unit and integration testing is in place to ensure these systems are communicating and storing data correctly.

Ensuring limited data retention
Doozy only retains data for as long as needed to fulfill contractual and regulatory requirements. Once that is no longer the case, data is deleted within 30 days.

Regular data audits are performed to ensure data is not being stored for longer than necessary.

Ensuring accountability
We maintain accountability by assigning clear roles and responsibilities for data protection, conducting regular audits, and adhering to data protection regulations.

Allowing data portability and erasure
Customers can request an export of their data which will be provided in a machine-readable format (JSON) made available to them securely within 30 days of request.

Data erasure requests are honored within 10 days, ensuring data is securely deleted in compliance with GDPR.