Emplify

Data Processing Agreement

This policy was last updated and released in July 2025.

Welcome to Breinchild Innovations Group Limited (**We**, Us, Our, Breinchild, the **Processor**)

You the Customer, the **Controller**

Breinchild recognises that some of our Customers' team members maybe subject to EU General Data Protection Regulation. Where such circumstances prevail, or there is a data transfer between EEA, UK, US, NZ and Australia, they will be subject to this Data Processing Agreement (the **Agreement**).

The purpose of this Agreement is to outline the work to be carried out by the Processor in relation with the Agreement. This Agreement shall be deemed to take effect from the effective date from the Customer accepting our Master Services Agreement (**MSA**) and shall continue in full force and effect until termination of the MSA.

Processing of Personal Data

The Processor agrees to process the Personal Data only in accordance with Data Protection Legislation.

The Parties acknowledge that the Processor may process Personal Data on behalf of the Controller during the term of this Agreement. A description of that and the activities undertaken by the Processor are set out in **Schedule 1**.

The Processor agrees to -

a) Solely process the Personal Data for the purposes of fulfilling its obligations under this Agreement and in compliance with the Customer's written instructions as set out in this Agreement and as may be specified from time to time in writing by the Controller;
b) Notify the Controller immediately if any instructions of the Controller relating to the processing of Personal Data are unlawful;
c) Maintain appropriate safeguards and implement security measures to safeguard Personal Data as identified in **Schedule 2**;
d) Not engage with any Sub-Processor to carry out any processing of Personal Data without the prior written consent of the Controller (such consent not to be unreasonably withheld).
e) The Processor will ensure that any Sub-Processor that it uses has a similar data protection policy in place but shall not be liable for the Sub-Processor's compliance with Data Protection Legislation.
f) Assist the Customer in retrieval and/or deletion of any Member's Personal Data.
g) Assist the Customer as required pursuant to any Data Protection Legislation.

Members Rights

The Processor shall –

a) Promptly notify the Controller if it receives a request from a Member (**Member's Access Request**) under any Data Protection Legislation in respect of Personal Data; and

b) Ensure that it does not respond to that request except on the documented instructions of the Controller or as required by applicable Data Protection Legislation to which the Processor is subject, in which case the Processor shall to the extent permitted by applicable Data Protection Legislation inform the Controller of that legal requirement before the Processor responds to the request.

Data Breaches

The Processor shall without undue delay inform the Controller of any Data Security Breaches.

The Processor shall provide information and assistance upon request to enable the Controller to notify Data Security Breaches to the relevant authority pursuant to the relevant data protection agency and affected individuals and any other regulators to whom the Controller is required to notify any Data Security Breaches and remedy the same.

Deletion or Return of Data

Upon termination of this Agreement, at the choice of the Controller, the Processor shall delete securely or return all Personal Data to the Controller and delete all existing copies of the Personal Data unless and to the extent that the Processor is required to retain copies of the Personal Data in accordance as stated in our Terms and Conditions or the MSA.

Audits

Upon receiving reasonable notice (no less than 21 days), the Controller may audit the Processor's compliance with this Agreement. The Controller shall make reasonable endeavours to avoid causing any damage, injury or disruption to the Processor.

Data Transfer

The Customer acknowledges that Emplify data will be primarily stored on servers located in Sydney, Australia.

Except as required by our identified use of Sub-Processors (see **schedule 3**) the Processor agrees not to transfer or authorize the transfer of Personal Data outside of the Region, without the prior written consent of the Customer.

We reserve the right to make changes to our MSA and our Terms and Conditions with 30 days' notice to ensure that we comply with Data Protection Laws.

Governing Law And Jurisdiction

This Agreement is governed by the laws of New Zealand.

Definitions

Controller As defined in the GDPR as is a legal or natural person, an agency, a public authority, or any other body who, alone or when joined with others, determines the purposes of any personal data and the means of processing it.

Data Protection Legislation: Means New Zealand's Privacy Act 2020, Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

Data Security Breach: A breach of security leading to the unlawful or accidental alteration, destruction, unauthorised disclosure of, loss or access to the shared Personal Data.

Members: Employees of the Customer and has the meaning of "Data Subject" as per Data Protection Legislation.

Personal Data Any information that relates to an identified or identifiable living individual.

Processor As defined in the GDPR as is a legal or a natural person, agency, public authority, or any other body who processes personal data on behalf of a Controller.

Sub-Processor: Means any subcontractor/third party of the Processor.

Working Day: A day other than a Saturday, Sunday, or public holiday in New Zealand.

SCHEDULE 1

DATA PROCESSING ACTIVITIES
DESCRIPTION OF DATA

This Schedule 1 includes the processing activities carried out by the Processor as identified in the MSA and our General Terms and Conditions.

The following information is gathered from Members that are registered to use our services:

- First and last name
- Workplace email address
- Mobile phone number
- Job title
- Role category
- Identity/gender
- Age band
- Tenure/length of time in workplace
- Work location
- Working from home situation
- Profile picture
- Member access level
- Survey data – Members' perceptions of their organisation's innovation culture, which are aggregated and reported anonymously
- Posts – any news and opinion pieces created by Members on our platform
- Payment data – collected from the account owner acting on behalf of the organisation

CATEGORIES OF MEMBERS

The Controller has defined the following Member categories from whom the Personal Data as defined above will be collected.

Members who create an account with Breinchild.
Members designated with Admin rights, who can perform additional tasks.

LAWFUL BASIS OF DATA PROCESSING

The Controller has determined the following lawful basis/bases to process personal data under the Data Protection Act 2018/GDPR 2016 is based on:

Consent of the Members to process Personal Data for the purposes of providing the services to Customer in accordance with our Terms and Conditions, Privacy Policy and MSA.

Process	System	Category	Data Held	Sub Processors
Sign Up	Emplify	Member	Member's first and last name Member's workplace email address and/or mobile phone number Organisation name	AWS, SendGrid

			User name and password	
Reset Password	Emplify	Member	Password	AWS, SendGrid
Member Profile	Emplify	Member	Member’s first and last name Job title Profile picture	AWS
Organisation Profile	Emplify	Organisation	Organisation name Organisation type Organisation main location Organisation establishment date Organisation size (employee count by band)	AWS
Member Management	Emplify	Member	Member access level	AWS, SendGrid
Scan	Emplify	Member	First and last name Workplace email address Workplace job title Role category Identity/gender Age band Tenure/length of time in workplace Work location Working from home situation Survey data – Members’ perceptions of their organisation’s innovation culture, which are aggregated and reported anonymously	AWS
Payment	Emplify	Payment Details	Organisation Name (legal entity) Registered address Payer email address Credit card details – name, number, expiry date and CVC	Stripe

SCHEDULE 2

Safeguard and security measures performed by Emplify:

- Encryption of data in transit
- Aggregation and anonymisation of survey data for reporting purposes
- Operational monitoring and regular system maintenance

Safeguard and security measures performed on our behalf by AWS:

- Identity and access management
- Network security
- Web application firewall
- Distributed Denial of Service (DDOS) protection
- Continuous security auditing and assessment
- Regular system maintenance

Safeguard and security measures performed on our behalf by Stripe:

- Level 1 PCI compliance
- Tokenisation of payment information
- Encryption of payment related data in transit
- Continuous security auditing and assessment
- Payment fraud prevention
- Regular system maintenance

SCHEDULE 3

Purpose and location of Sub Processors:

Name	Purpose	Server Location(s)
AWS	Hosting & Infrastructure	Sydney, Australia
Stripe	Payment	International locations
SendGrid	Email Services	International locations